Staatsblad
van het Koninkrijk der Nederlanden

Jaargang 2011

15

Besluit van 17 januari 2011, houdende regels met betrekking tot het elektronisch proces-verbaal (Besluit elektronisch proces-verbaal)

Wij Beatrix, bij de gratie Gods, Koningin der Nederlanden, Prinses van Oranje-Nassau, enz. enz. enz.

Op de voordracht van Onze Minister van Justitie van 29 september 2010, nr. 5669201/10/6;
Gelet op artikel 153, tweede lid, van het Wetboek van Strafvordering;
De Raad van State gehoord (advies van 3 december 2010, nr. W03.10.0476/II);
Gezien het nader rapport van Onze Minister van Veiligheid en Justitie van 22 december 2010, nr. 5678816/10/6;

Hebben goedgevonden en verstaan:

Artikel 1

In dit besluit wordt verstaan onder:
a. *elektronisch proces-verbaal:* proces-verbaal, bedoeld in artikel 152 en 153, eerste lid, van het Wetboek van Strafvordering, dat langs elektronische weg is opgemaakt of dat langs elektronische weg is omgezet in een digitaal afschrift;
b. *digitaal afschrift:* elektronisch gegevensbestand dat een identieke weergave vormt van het proces-verbaal, bedoeld in artikel 153, eerste lid en tweede lid, eerste volzin, van het Wetboek van Strafvordering;
c. *validatie:* vaststelling van de geldigheid van een elektronische handtekening, door het verifiëren van de geldigheid van het certificaat gerelateerd aan het moment van ondertekening en het verifiëren van de ongewijzigde staat van het document aan de hand van de ondertekening;
d. *elektronische handtekening:* de handtekening, bedoeld in artikel 15a, vierde lid, van Boek 3 van het Burgerlijk Wetboek;
e. *gekwalificeerde elektronische handtekening:* elektronische handtekening gebaseerd op een gekwalificeerd certificaat en gegenereerd door een veilig middel voor het aanmaken van elektronische handtekeningen overeenkomstig de eisen, gesteld in artikel 15a, tweede lid, onderdelen a tot en met f, van Boek 3 van het Burgerlijk Wetboek;
f. *elektronische dagtekening:* een tijdstempel dat de datum en het tijdstip vermeldt van het moment van ondertekenen van een elektronisch proces-verbaal en dat is afgegeven overeenkomstig geldende normen en standaarden;
g. *certificaat, gekwalificeerd certificaat, certificatiedienstverlener en*

veilig middel voor het aanmaken van elektronische handtekeningen: het certificaat, het gekwalificeerd certificaat, de certificatiedienstverlener, respectievelijk het veilig middel voor het aanmaken van elektronische handtekeningen, bedoeld in artikel 1.1, onderdelen ss, tt, uu, respectievelijk ww, van de Telecommunicatiewet.

h. *verantwoordelijke:* het hoofd van de organisatie waar een ambtenaar werkzaam is die een elektronisch proces-verbaal opmaakt of ontvangt of een digitaal afschrift vervaardigt of ontvangt.

Artikel 2

1. Een elektronisch proces-verbaal is voorzien van een elektronische dagtekening en een gekwalificeerde elektronische handtekening, in een documentformaat dat voldoet aan het bij of krachtens de Archiefwet 1995 bepaalde.

2. Als een elektronisch proces-verbaal wordt tevens aangemerkt een digitaal afschrift dat is voorzien van een gekwalificeerde elektronische handtekening van een, daartoe door de verantwoordelijke aangewezen, ambtenaar als waarmerk, overeenkomstig de eisen, bedoeld in het eerste lid.

Artikel 3

1. In aanvulling op de gegevens die op grond van artikel 3 van het Besluit elektronische handtekeningen in het gekwalificeerd certificaat zijn opgenomen, worden gegevens opgenomen over de organisatie waar de ambtenaar, aan wie het betreffende certificaat is afgegeven, werkzaam is.

2. In afwijking van artikel 3, onderdeel c, van het Besluit elektronische handtekeningen kan van een pseudoniem slechts in bijzondere gevallen gebruik worden gemaakt.

Artikel 4

1. Een proces-verbaal wordt uitsluitend omgezet in een digitaal afschrift met toepassing van de voorschriften voor een identieke weergave, omschreven in de bijlage I bij dit besluit.

2. In een digitaal afschrift wordt vermeld dat het een identieke weergave en kopie is van het proces-verbaal.

3. Bij ministeriële regeling kunnen nadere regels worden gesteld betreffende de voorschriften, bedoeld in het eerste lid.

Artikel 5

1. De verantwoordelijke bewaart over de elektronische handtekening en dagtekening de in bijlage II bij dit besluit omschreven gegevens met het oog op de validatie.

2. De gegevens, bedoeld in het eerste lid, worden tezamen met het elektronisch proces-verbaal bewaard gedurende de periode van bewaring van het elektronisch proces-verbaal.

3. De gegevens, bedoeld in het tweede lid, worden op zodanige wijze bewaard dat op ieder moment de ongewijzigde staat daarvan kan worden aangetoond.

Artikel 6

1. De verantwoordelijke die een elektronisch proces-verbaal heeft ontvangen verzendt onmiddellijk een bevestiging van ontvangst aan de verantwoordelijke die dit proces-verbaal heeft verzonden.

2. De verantwoordelijke die het elektronisch proces-verbaal heeft verzonden bewaart de bevestiging van ontvangst, bedoeld in het eerste lid, gedurende een periode van vijf jaar.

3. De verantwoordelijke die een elektronisch proces-verbaal heeft ontvangen, zorgt ervoor dat dit onverwijld wordt gevalideerd.

4. Indien de validatie uitwijst dat de gecontroleerde waarden niet overeen komen, dan wordt dit onverwijld bericht aan de verantwoordelijke, die het elektronisch proces-verbaal heeft verzonden.

5. Indien er aanwijzingen zijn dat een digitaal afschrift geen identieke weergave vormt van het proces-verbaal dan wordt dit onverwijld aan de verantwoordelijke bericht, die het digitaal afschrift heeft verzonden.

6. De verantwoordelijke, die een elektronisch proces-verbaal heeft verzonden en aan wie een bericht is verzonden dat de gecontroleerde waarden niet overeen komen of dat een digitaal afschrift geen identieke weergave vormt van het proces-verbaal, is gehouden te voorzien in een elektronisch proces-verbaal dan wel een digitaal afschrift, overeenkomstig de eisen van dit besluit.

Artikel 7

1. De verantwoordelijke treft technische en organisatorische maatregelen om het elektronisch proces-verbaal en de gegevens, bedoeld in de artikelen 4, 5 en 6, te beveiligen tegen misbruik, verlies, of onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau, gelet op de risico's die de verwerking en de aard van de gegevens met zich meebrengen.

2. Het elektronisch proces-verbaal en de gegevens, bedoeld in de artikelen 4, 5 en 6, zijn uitsluitend toegankelijk voor personen die daarvoor zijn geautoriseerd.

Artikel 8

Dit besluit wordt aangehaald als: Besluit elektronisch proces-verbaal.

Artikel 9

Dit besluit treedt in werking op een bij koninklijk besluit te bepalen tijdstip.

Het advies van de Afdeling advisering van de Raad van State wordt met de daarbijbehorende stukken openbaar gemaakt door publicatie in de Staatscourant.

Lasten en bevelen dat dit besluit met de daarbij behorende nota van toelichting in het Staatsblad zal worden geplaatst.

's-Gravenhage, 17 januari 2011

Beatrix

De Minister van Veiligheid en Justitie,
I. W. Opstelten

Uitgegeven de *zesentwintigste* januari 2011

De Minister van Veiligheid en Justitie,
I. W. Opstelten

STB13846
ISSN 0920 - 2064
's-Gravenhage 2011

Bijlage I, bedoeld in artikel 4 van het Besluit elektronisch proces-verbaal

Voorschriften voor de omzetting van een proces-verbaal in een digitaal afschrift:

1. Van de omzetting van het proces-verbaal of enig ander document in het strafproces in een digitaal afschrift is slechts sprake indien de omzetting geschiedt met een juiste en volledige weergave van de in het om te zetten proces-verbaal of enig ander document voorkomende gegevens.
2. De verantwoordelijkheden en bevoegdheden binnen de organisatie ten aanzien van het proces van omzetting zijn vastgelegd en vastgesteld. Hierin zijn opgenomen de criteria voor en de frequentie van interne controles op het omzettingsproces.
3. Ten aanzien van het proces-verbaal of enig ander document in het strafproces wordt minimaal vastgelegd: de wijze waarop deze worden ontvangen en de wijze waarop de gescande documenten in enig systeem worden opgenomen.
4. Ten aanzien van de hardware worden de specificaties van de scanner vastgelegd.
5. Ten aanzien van de software wordt vastgelegd:
a. de naam van het softwarepakket;
b. het versienummer;
c. de releasedatum;
d. de leverancier;
e. voor zover van toepassing: de geïnstalleerde service packs of patches.
6. Scanning geschiedt in kleur.
7. Het digitale beeld wordt opgeslagen in een gestandaardiseerd, apparaatonafhankelijk kleurenprofiel.
8. Als scanparameter geldt 300 dpi met bitdiepte 24.
9. Ten aanzien van het bestandsformaat wordt gebruik gemaakt van zogenaamde open standaarden. Dit zijn standaarden die via een formeel en open proces binnen een erkend standaardisatieorgaan (bijvoorbeeld ISO, NEN, W3C) tot stand komen.
10. Indien bij het scanproces gebruik wordt gemaakt van een tussenformaat, dan mag geen kwaliteitsverlies optreden bij de omzetting van het tussenformaat naar het uiteindelijke formaat.

Bijlage II, bedoeld in artikel 5 van het Besluit elektronisch proces-verbaal

In deze bijlage wordt verstaan onder[1]:

Veilig middel (ook wel SSCD of Secure Signature Creation Device): Een middel voor het aanmaken van elektronische handtekeningen dat voldoet aan de eisen gesteld krachtens artikel 18.17, eerste lid van de Telecommunicatiewet (definitie Wet elektronische handtekeningen). Binnen de PKI voor de overheid is in domein Burger gekozen voor de smartcard als SSCD. In domein Overheid en Bedrijven kunnen zowel smartcards als USB-tokens worden gebruikt, mits deze aan de gestelde eisen voldoen.

Hash algoritme: Een functie die een bericht van willekeurige lengte omzet in een reeks met een vaste lengte en voldoet aan de volgende voorwaarden:

• Het is praktisch onuitvoerbaar om voor een gegeven uitvoer een invoer te vinden die deze uitvoer als resultaat heeft;

• Het is praktisch onuitvoerbaar om voor een gegeven invoer een tweede invoer te vinden die dezelfde uitvoer als resultaat heeft;

• Het is praktisch onuitvoerbaar om twee willekeurige berichten te vinden die dezelfde uitvoer als resultaat hebben;

(Voorbeelden zijn SHA-1 of SHA-2 of RIPEMD-160).

Encryptie: Een proces waarmee gegevens met behulp van een wiskundig algoritme en een cryptografische sleutel worden vercijferd, zodat deze onleesbaar worden voor onbevoegden.

De betrouwbaarheid van de encryptie hangt af van het algoritme, de implementatie daarvan, de lengte van de cryptografische sleutel en de gebruiksdiscipline. Bij symmetrische encryptie wordt bij het vercijferen en ontcijferen gebruik gemaakt van één en dezelfde, geheime, sleutel. Bij asymmetrische encryptie wordt gebruik gemaakt van een sleutelpaar. De ene sleutel, de private sleutel, is slechts bekend bij de eindgebruiker van deze sleutel en moet strikt geheim worden gehouden. De andere, de publieke sleutel, wordt verspreid onder communicatiepartners. Wat met de private sleutel is vercijferd, kan alleen met de bijbehorende publieke sleutel worden ontcijferd, en omgekeerd.

De onderstaande gegevens hebben tot doel om de geldigheid en ongewijzigde toestand aan te tonen, ongeacht het tijdstip waarop dit wordt gevraagd, van de elektronische handtekening in relatie tot het document, de gehanteerde certificaten, de gegevens omtrent de ondertekenaar(s) van het document en het tijdstip van de ondertekening(en);

A. Gegevens omtrent het certificaat dat gebruikt is voor een elektronische handtekening:

a. het publieke certificaat van de elektronische handtekening;

b. de identificerende gegevens van het certificaat;

c. de naam van de ondertekenaar zoals dat opgegeven is in het certificaat;

d. de naam van de organisatie waartoe de ondertekenaar behoort;

e. de identificatie en het land van vestiging van de afgevende certificatiedienstverlener(s);

f. de vermelding van de tijdstippen van het begin en van het einde van de geldigheidsduur van het certificaat;

g. het tijdstip waarop de elektronische handtekening geplaatst is op basis van de elektronische dagtekening zoals die bij de handtekening gevoegd is op het moment van ondertekenen;

h. alle certificaten, tot en met het stamcertificaat, waaruit de geldigheid van het onderhavige certificaat blijkt;

[1] Begrippenlijst PKIoverheid, april 2010 (http://www.logius.nl/nc/begrippenlijst).

i. de antwoorden van de certificatiedienstverlener(s) waaruit de geldigheid blijkt van alle certificaten zoals die gebruikt zijn op het moment van ondertekenen, overeenkomstig de geldende normen en standaarden, rekening houdend met de door een certificatiedienstverlener bekend gestelde tijdsduur tussen een verzoek tot intrekking van een gekwalificeerd certificaat tot een publicatie van die intrekking;

j. gegevens over de gehanteerde certificaat versie, het gehanteerde hash algoritme en het gehanteerde encryptie algoritme van ieder certificaat;

k. een aanduiding of het certificaat een gekwalificeerd certificaat is of een andersoortig certificaat;

l. een aanduiding of de handtekening door een veilig middel is aangemaakt.

B. Gegevens omtrent het certificaat dat gebruikt is voor het plaatsen van de elektronische dagtekening, behorende bij een elektronische handtekening:

a. het publieke certificaat van de elektronische dagtekening;

b. de identificerende gegevens van het certificaat;

c. alle certificaten, tot en met het stamcertificaat, waaruit de geldigheid van het certificaat blijkt dat gebruikt is voor het plaatsen van de dagtekening;

d. de antwoorden van de certificatiedienstverlener(s) waaruit de geldigheid blijkt van alle certificaten zoals die gebruikt zijn op het moment van de dagtekening, overeenkomstig de geldende normen en standaarden, rekening houdend met de door een certificatiedienstverlener bekend gestelde tijdsduur tussen een verzoek tot intrekking van een gekwalificeerd certificaat tot een publicatie van die intrekking;

e. gegevens over de gehanteerde certificaat versie, het gehanteerde hash algoritme en het gehanteerde encryptie algoritme van ieder certificaat;

f. een aanduiding of het certificaat een gekwalificeerd certificaat is of een andersoortig certificaat;

g. een aanduiding of het certificaat door een veilig middel is aangemaakt.

C. Gegevens omtrent de ondertekening van het document:

a. voor zover beschikbaar de gegevens omtrent de plaats van de ondertekening, de rol van de ondertekenaar en de reden van de ondertekening;

b. voor zover beschikbaar overige informatie voor een eenduidige interpretatie op basis waarvan een elektronische handtekening is geplaatst en naderhand is gevalideerd;

D. Gegevens omtrent het moment waarop de validatie werd uitgevoerd:

a. het tijdstip, op basis van een vertrouwd tijdstempel, waarop de verificatie heeft plaatsgevonden, tot op de minuut nauwkeurig;

b. voor zover beschikbaar gegevens over de persoon of instantie die de verificatie uitvoert;

c. voor zover beschikbaar de rol van de persoon of instantie die de verificatie uitvoert;

E. Gegevens omtrent de waarborgen van de integriteit van de validatie gegevens (A tot en met D) en het elektronisch proces-verbaal:

a. een verifieerbaar tijdstip waarop de gegevens beschermd zijn tegen wijzigingen;

b. de gehanteerde algoritmen waarmee de gegevens beschermd zijn tegen wijzigingen;

c. een aanduiding voor de methodiek die gehanteerd is; deze methodiek zal elders moeten zijn gedocumenteerd;

d. gegevens waarmee de integriteit geverifieerd kan worden.

NOTA VAN TOELICHTING

Algemeen deel

1. Inleiding

De ontwikkelingen op het gebied van de informatisering maken het eenvoudig om documenten langs elektronische weg te verzenden. Dit is ook voor de strafrechtspleging van belang, omdat het papieren proces-verbaal en het papieren dossier kunnen worden vervangen door een proces-verbaal en een dossier in elektronische vorm. Hiermee kunnen efficiencyvoordelen worden behaald, omdat de administratieve verwerking eenvoudiger wordt. Daarnaast wordt het risico op vertraging of zelfs mislukking van een strafprocedure vanwege het zoekraken van documenten geminimaliseerd, omdat het mogelijk is om op basis van het elektronische gegevensbestand een identiek afschrift van de originele documenten te vervaardigen.

Inmiddels is het wettelijk mogelijk om langs elektronische weg aangifte van strafbare feiten te doen. Dit is geregeld met de Wet van 15 september 2005 tot wijziging van het Wetboek van Strafvordering (elektronische aangiften en processen-verbaal)[1]. De aan de elektronische aangifte te stellen eisen zijn inmiddels uitgewerkt in het Besluit elektronische aangifte. Het Besluit elektronische aangifte is, tezamen met de betreffende onderdelen van de Wet elektronische aangiften en processen-verbaal, in december 2006 in werking getreden[2]. Hiermee wordt de mogelijkheid geboden langs elektronische weg aangifte te doen van een beperkt aantal strafbare feiten. De technische voorziening daarvoor is op dit moment echter nog niet goedgekeurd.

Met de Wet elektronische aangiften en processen-verbaal is het daarnaast wettelijk mogelijk gemaakt een proces-verbaal langs elektronische weg op te maken. De wet voorziet erin dat met een ondertekend proces-verbaal wordt gelijkgesteld een proces-verbaal dat langs elektronische weg is opgemaakt en verzonden, mits dit voldoet aan de bij of krachten algemene maatregel van bestuur gestelde eisen (art. I, onderdeel A, van de Wet elektronische aangiften en processen-verbaal). De aan het elektronisch proces-verbaal te stellen eisen worden in dit besluit uitgewerkt.

De eisen aan het elektronisch proces-verbaal dienen om de authenticiteit en de integriteit van het proces-verbaal te waarborgen. De authenticiteit verzekert dat de betreffende opsporingsambtenaar het elektronisch proces-verbaal daadwerkelijk heeft opgesteld en ondertekend. De integriteit verzekert dat de inhoud van het betreffende proces-verbaal na de ondertekening niet is gewijzigd. Zekerheid over de authenticiteit en integriteit van een proces-verbaal zijn essentieel vanwege de betekenis van een proces-verbaal in het strafproces. Een proces-verbaal van een opsporingsambtenaar heeft een zelfstandige bewijskracht; het bewijs dat de verdachte het tenlastegelegde feit heeft gepleegd, kan door de rechter worden aangenomen op het proces-verbaal van een opsporingsambtenaar (art. 344, tweede lid, Sv).

2. De reikwijdte van de regeling

Dit besluit heeft betrekking op het proces-verbaal van opsporingsambtenaren «van het door hen opgespoorde strafbare feit of van hetgeen door hen tot opsporing is verricht of bevonden» (art. 152 Sv). In het strafproces komen ook andere processen-verbaal voor, bijvoorbeeld het proces-verbaal van een terechtzitting (art. 326 en 327 Sv), maar dit besluit beperkt

[1] Stb. 2005, 470.
[2] Stb. 2006, 727 en 728.

zich tot de in artikel 152 van het Wetboek van Strafvordering bedoelde processen-verbaal. Het proces-verbaal wordt door hen persoonlijk opgemaakt, gedagtekend en ondertekend (art. 153 Sv). Zoals in de memorie van toelichting bij de Wet elektronische aangiften en processen-verbaal is aangegeven, zal de wenselijkheid en mogelijkheid van een meer omvattende regeling van het elektronisch verkeer in het strafprocesrecht nader moeten worden bezien, zonodig in het kader van de modernisering van het Wetboek van Strafvordering, zodat rekening kan worden gehouden met de ervaringen die met die wet zijn opgedaan (Kamerstukken II, 2003/04, 29 438, nr. 3, blz. 2/3).

Dit besluit heeft betrekking op het proces-verbaal van een opsporingsambtenaar. Dit betreft in de eerste plaats ambtenaren met algemene opsporingsbevoegdheid. Daartoe behoren de ambtenaren van de politie en van de Koninklijke marechaussee, die zijn belast met de uitvoering van de politietaak, als bedoeld in de artikelen 2 en 6 van de Politiewet 1993. Daartoe behoren ook de opsporingsambtenaren van de bijzondere opsporingsdiensten en de officieren van justitie (art. 141 Sv). Dit betreft in de tweede plaats buitengewone opsporingsambtenaren. Daartoe behoren de personen aan wie een akte van opsporingsbevoegdheid is verleend, de opsporingsbevoegdheid strekt zich dan uit tot de in de akte of aanwijzing aangeduide strafbare feiten. Daartoe behoren tevens de personen die bij bijzondere wetten met de opsporing van de daarin bedoelde strafbare feiten zijn belast (art. 142, eerste lid, Sv).

Dit besluit heeft betrekking op het proces-verbaal dat in elektronische vorm wordt opgemaakt. Daarvan kan een afschrift worden gemaakt, in papieren vorm. Voor de rechtsgeldigheid van een elektronisch proces-verbaal is het echter niet nodig, en zelfs niet wenselijk, dat het elektronisch proces-verbaal wordt uitgeprint en ondertekend. Dan zou er immers nog steeds sprake zijn van de noodzaak om een papieren proces-verbaal op te maken en te ondertekenen. Met het vereiste van een elektronische handtekening kan worden gewaarborgd dat een proces-verbaal, dat langs elektronische weg is opgemaakt, voldoet aan de eisen van authenticiteit en integriteit.

Andersom is het mogelijk een papieren proces-verbaal te scannen en om te zetten in een elektronisch bestand. Het elektronische bestand vormt dan een afschrift in elektronische vorm, oftewel een «digitaal afschrift», van het papieren proces-verbaal. Met een elektronische handtekening als waarmerk wordt door de ondertekenaar aangegeven en waarborgd dat het elektronische bestand een identieke weergave is van het originele papieren proces-verbaal. Dit is van groot belang voor de instanties, die zijn betrokken bij de rechtshandhaving, omdat langs deze weg een papieren proces-verbaal in een later stadium alsnog kan worden omgezet in een digitaal afschrift. Daarom zijn in dit besluit tevens eisen opgenomen voor het digitaal afschrift, dat het resultaat is van het omzetten van een papieren proces-verbaal en dat is voorzien van een elektronische handtekening zodat dit afschrift dezelfde bewijskracht kan toekomen als het originele papieren proces-verbaal.

3. Uitgangspunten voor de regeling

Een belangrijk uitgangspunt voor de regels in dit besluit is dat zoveel mogelijk bij de bestaande wettelijke regels en beleidsontwikkelingen wordt aangesloten. Deze regels hebben betrekking op de betrouwbaarheid van een elektronische handtekening en de bewaring en archivering van processen-verbaal. De beleidsontwikkelingen betreffen de digitalisering van de informatiehuishouding bij politie en justitie en de uitgifte van de Rijkspas en de elektronische identiteitskaart (eNIK). Dit wordt hieronder nader toegelicht.

Ter implementatie van Richtlijn 1999/93/EG, van 13 december 1999[1], bevat het Burgerlijk Wetboek een regeling voor de elektronische handtekening. Bij de uitwerking van de eisen voor de betrouwbaarheid wordt onderscheid gemaakt tussen de «gewone» elektronische handtekening, de geavanceerde elektronische handtekening en de gekwalificeerde elektronische handtekening, afhankelijk van het niveau van betrouwbaarheid. De regeling van het Burgerlijk Wetboek geldt in beginsel uitsluitend voor het civiele recht, maar de wet bevat een zogenaamde schakelbepaling. De regeling van de elektronische handtekening is hierdoor ook buiten het vermogensrecht van overeenkomstige toepassing, voorzover de aard van de rechtshandeling of van de rechtsbetrekking zich daartegen niet verzet (art. 3:15c BW). In de memorie van toelichting is aangegeven dat met die ruimere werking ook wordt gedoeld op mogelijke toepassing van de elektronische handtekening in het bestuursrecht en het strafrecht. Voor deze rechtsgebieden zal afzonderlijk worden bekeken of, en zo ja in welke gevallen rechtsverkeer tussen overheid en burger langs elektronische weg zal kunnen plaatsvinden en of daarvoor aanvullende eisen noodzakelijk zijn. De Wet elektronisch bestuurlijk verkeer, die voorziet in een aanvulling van de Algemene wet bestuursrecht, is daarvan een uitvloeisel.

Op 1 juli 2010 is de Wet elektronisch verkeer met de bestuursrechter in werking getreden. Deze wet behelst een regeling voor het elektronisch verkeer met de bestuursrechter, in aanvulling op de regeling in de Algemene wet bestuursrecht over het verkeer langs elektronische weg tussen burgers en bestuursorganen (Afdeling 2.3. Awb). Voor de ondertekening van stukken wordt in de Wet elektronisch verkeer met de bestuursrechter eveneens aangesloten bij de regeling van de elektronische handtekening van het Burgerlijk Wetboek.

Het ligt voor de hand om voor het proces-verbaal van een opsporingsambtenaar uit te gaan van de regeling van de elektronische handtekening van het Burgerlijk Wetboek. De regeling wordt in het civiele recht reeds langere tijd toegepast en wordt nu tevens gebruikt in het bestuursrecht. De regeling is goed toepasbaar voor het elektronisch proces-verbaal omdat een document, nadat dit met een elektronische handtekening is ondertekend, als het ware wordt «verzegeld». Met de elektronische handtekening wordt een unieke hash-waarde[2] aan het document toegekend en ondertekend; bij iedere wijziging of andere mutatie van een document verandert de hash-waarde. Uitgangspunt is dat de hash-waarde na de ondertekening niet meer verandert, daardoor kan de integriteit van een elektronisch proces-verbaal in een later stadium worden aangetoond op basis van de ondertekening.

Binnen de overheid is een afsprakenstelsel ontwikkeld voor de certificaatdienstverlening via het internet. Het programma PKIoverheid («Public Key Infrastructure voor de overheid») bestaat uit organisatorische en technische componenten die een beveiligde communicatie mogelijk maken. Daarbij wordt uitgegaan van de eisen van het Burgerlijk Wetboek. Aanvullend worden nadere eisen gesteld om de betrouwbaarheid van de infrastructuur voor de overheid te waarborgen. Deze eisen hebben onder meer betrekking op de certificaten en de aanbieders van die certificaten.

Omdat dit besluit voorziet in de mogelijkheid dat het proces-verbaal van een opsporingsambtenaar tussen overheidsorganisatie wordt uitgewisseld, wordt uitgegaan van de eisen van PKI-overheid.

Een belangrijk aspect betreft de bewaring en archivering van een elektronisch proces-verbaal. Daarbij zijn ook regels op het gebied van de beveiliging en de bescherming van de persoonlijke levenssfeer aan de orde. Voor papieren processen-verbaal zijn dergelijke regels reeds van kracht. De Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens geven regels voor de zorgvuldige gegevensverwerking. De

[1] PbEG L 13.
[2] Zie hiervoor de toelichting bij artikel 1, onderdeel c.

Archiefwet geeft regels voor de archivering en opslag van een proces-verbaal. Voor de beveiliging van de gegevens zijn het Voorschrift Informatiebeveiliging Rijksdienst (VIR) en de Regeling informatiebeveiliging politie van belang. Deze wetten en regels maken geen onderscheid in de vorm waarin de gegevens worden verwerkt, en zijn onverkort van toepassing op de gegevens van een elektronisch proces-verbaal.

Voorkomen moet worden dat nieuwe regels worden gesteld voor het elektronisch proces-verbaal, waardoor overlap kan ontstaan met de bestaande regels voor een proces-verbaal. Uitgangspunt van dit besluit is dat met de aanvullende regels voor het elektronisch proces-verbaal nauw wordt aangesloten op de bestaande voorschriften op het gebied van beveiliging en opslag van een proces-verbaal, en wel op zodanige wijze dat de regels van dit besluit als het ware een schil vormen rondom de bestaande voorschriften. Op een enkel punt zijn «dubbele regels» echter niet te voorkomen, zoals bijvoorbeeld bij de bewaring van een papieren proces-verbaal nadat dit is gescand en aldus is omgezet in een digitaal afschrift. Bij ontstentenis van voldoende ervaring met dit proces verzet het belang van de rechtszekerheid zich vooralsnog tegen de vernietiging van een papieren proces-verbaal, nadat dit in een digitaal afschrift is omgezet en van een elektronische handtekening is voorzien. Dit wordt hieronder, in paragraaf 6, toegelicht.

Binnen de Nederlandse politie is het Digitaal Procesdossier Loopzaken (DPL) in ontwikkeling, dat voorziet in de mogelijkheid tot het langs elektronische weg opstellen en verzenden van een proces-verbaal. Door het openbaar ministerie en de zittende magistratuur wordt thans gewerkt aan de invoering van het Geïntegreerd Processysteem Strafrecht (GPS) dat voorziet in vervanging van het papieren strafdossier door een elektronisch (of digitaal) strafdossier. Daarmee zullen op papier vastgelegde en van handgeschreven handtekeningen voorziene beschikkingen, bevelen, processen-verbaal en andere geschriften gaandeweg tot het verleden gaan behoren.

Uitgangspunt van dit besluit is dat de regels voor het elektronische proces-verbaal passen binnen de ontwikkelingen op het gebied van de informatiehuishouding binnen de strafrechtsketen, met name bij de politie en de rechterlijke macht.

Met de regels van dit besluit wordt aangesloten bij rijksbrede ontwikkelingen zoals de uitgifte van de Rijkspas en de elektronische identiteitskaart (eNIK). Beide passen worden uitgegeven via een gekwalificeerd proces en voldoen aan de eisen die aan een veilig middel worden gesteld. Aldus kunnen deze passen als een veilig middel in de zin van de Telecommunicatiewet worden aangemerkt, zodat een opsporingsambtenaar van de politie een van deze passen kan gebruiken ten behoeve van het opmaken en verzenden van een elektronisch proces-verbaal, conform de eisen van dit besluit. Ditzelfde geldt voor een ambtenaar van het openbaar ministerie, die een digitaal afschrift van een elektronische handtekening voorziet. Zowel de Rijkspas als de eNIK beschikken (nog) niet over een certificaat waarmee elektronische handtekeningen kunnen worden geplaatst. Maar vanwege het gekwalificeerde karakter van de passen, kunnen de tekencertificaten door middel van een betrekkelijk eenvoudige procedure worden bijgeplaatst. Hiermee zullen de kosten van de invoering van het elektronisch proces-verbaal binnen de strafrechtsketen sterk worden gereduceerd.

Waar nodig zal in de navolgende paragrafen nader worden ingegaan op de bestaande wetten en regels, of initiatieven op het gebied van het beleid, die raakvlakken hebben met de invoering van het elektronisch proces-verbaal binnen de strafrechtsketen.

4. De regeling van de elektronische handtekening in het Burgerlijk Wetboek en de toepassing van die regeling voor het elektronisch proces-verbaal

In het Burgerlijk Wetboek is geregeld dat een elektronische handtekening dezelfde rechtsgevolgen heeft als een handgeschreven handtekening indien de methode die daarbij is gebruikt voor authentificatie voldoende betrouwbaar is, gelet op het doel waarvoor de elektronische gegevens werden gebruikt en op alle overige omstandigheden van het geval (art. 3:15a, eerste lid, BW). De eisen met betrekking tot de betrouwbaarheid zijn uitgewerkt in het tweede lid, onderdelen a tot en met d, van voormeld artikel. De handtekening dient op unieke wijze aan de ondertekenaar te zijn verbonden, het mogelijk te maken de ondertekenaar te identificeren, tot stand te komen met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden en op zodanige wijze aan het betreffende elektronische bestand te zijn verbonden dat elke wijziging achteraf van de gegevens kan worden opgespoord.

De elektronische handtekening die aan deze eisen voldoet wordt aangeduid als de geavanceerde elektronische handtekening. Een veel gebruikte techniek voor het aanmaken van een geavanceerde elektronische handtekening is gebaseerd op het gebruik van twee codes die onlosmakelijk aan elkaar zijn verbonden: een publieke en een private sleutel. Deze sleutels zijn uniek voor een persoon. Welke publieke sleutel bij welke persoon hoort, wordt door een certificatiedienstverlener (hierna ook te noemen: CSP) vastgelegd in een (digitaal) certificaat. De betreffende persoon kan een elektronisch bestand ondertekenen met zijn private sleutel. De ontvanger van dit bestand kan alleen met de bijbehorende publieke sleutel verifiëren of het bericht ongewijzigd is en afkomstig van de bezitter van de bijbehorende (geheime) private sleutel. De private sleutel is uniek voor de ondertekenaar en mag niet bekend raken bij anderen. Om de private sleutel onder zijn uitsluitende controle te kunnen houden zijn er diverse (combinaties van) mogelijkheden. Om te kunnen voldoen aan het vereiste dat de ondertekenaar geïdentificeerd kan worden moet de ontvanger weten welke publieke sleutel bij welke verzender hoort. Deze informatie staat op het certificaat dat door de certificatiedienstverlener voor de ondertekenaar is afgegeven en wordt bijgevoegd bij de ondertekening.

Daarnaast wordt in het Burgerlijk Wetboek de mogelijkheid geboden voor een elektronische handtekening die is gebaseerd op een gekwalificeerd certificaat en is gegenereerd door een veilig middel voor het aanmaken van elektronische handtekeningen (art. 3:15a, tweede lid, BW). Een elektronische handtekening die aan deze aanvullende eisen voldoet, wordt aangeduid als een gekwalificeerde elektronische handtekening. De gekwalificeerde elektronische handtekening kent gestandaardiseerde veiligheidswaarborgen voor de geavanceerde elektronische handtekening. Met de aanvullende eisen wordt voorkomen dat ingewikkelde technische en juridische discussies kunnen ontstaan over de beoordeling en interpretatie van een geavanceerde handtekening. Het zogenaamde veilig middel zorgt ervoor dat het certificaat niet gedupliceerd kan worden, waardoor het gebruik van het certificaat beperkt wordt tot de persoon die het veilig middel in zijn bezit heeft en de toegangscode (pincode) kent; de ondertekenaar. De eisen voor het certificaat en voor het veilig middel zijn opgenomen in de Telecommunicatiewet (artikelen 18.15 en 18.17 Tw) en uitgewerkt in het Besluit elektronische handtekeningen en de Regeling elektronische handtekeningen. Deze eisen hebben betrekking op de certificatiedienstverlener, het certificaat, het veilig middel voor het aanmaken van elektronische handtekeningen en de beoordeling van het veilig middel door een daartoe door Onze Minister van Economische

Zaken aangewezen instelling. Certificatiedienstverleners moeten zijn geregistreerd bij de Onafhankelijke Post- en Telecommunicatie Autoriteit (OPTA). Gekwalificeerde certificaten kunnen overigens onafhankelijk van veilige middelen worden uitgegeven. Als veilig middel in de zin van de wet geldt een gecertificeerde smartcard of een USB-token.

In lijn met de eerdergenoemde Europese richtlijn is in het Burgerlijk Wetboek bepaald dat de methode voor authentificatie niet als onvoldoende betrouwbaar kan worden aangemerkt op de enkele grond dat deze niet is gebaseerd op een certificaat of een veilig middel, dat aan de in de Telecommunicatiewet gestelde eisen voldoet (art. 3:15a, derde lid, BW). Deze regel biedt een opening om een elektronische handtekening, die niet aan de bovenvermelde wettelijke eisen voldoet, alsnog rechtsgeldig te achten. Dit vereist echter aanvullend bewijs.

Het is een logische keuze om voor het niveau van bescherming en beveiliging van het elektronisch proces-verbaal aan te sluiten bij het Burgerlijk Wetboek. Voor zowel het burgerlijk bestuursrecht en het strafrecht geldt dan een uniforme regeling. Meer praktisch betekent deze keuze dat aangesloten wordt bij een set van beproefde internationale en Europese standaarden omtrent de uitgifte en het beheer van veiligheidssleutels en de toepassing van encryptische technologie. Daarbij gaat de voorkeur uit naar het hoogste niveau van betrouwbaarheid. Een proces-verbaal wordt op ambtseed opgemaakt en dient als bewijsmiddel in het strafproces. Het ligt dan ook voor de hand dat de betrouwbaarheid van het elektronisch proces-verbaal boven iedere twijfel dient te zijn verheven. Dit impliceert dat de hoogste eisen worden gesteld ten aanzien van het proces door middel waarvan het proces-verbaal tot stand komt en waarmee uiteindelijk de authenticiteit en de integriteit van het proces-verbaal worden gerealiseerd. Daarom wordt met dit besluit gekozen voor de gekwalificeerde elektronische handtekening voor het elektronisch proces-verbaal.

De uitzonderingsclausule van artikel 3:15a, derde lid, BW, voor de elektronische handtekening in het civiele recht, is niet van toepassing. De reden daarvoor is, zoals hierboven uiteengezet, dat een dergelijke uitzonderingsclausule met het oog op de functie van het proces-verbaal als bewijsmiddel in het strafproces, niet goed verenigbaar is met de behoefte aan een heldere norm die de authenticiteit en integriteit van het elektronisch proces-verbaal buiten twijfel stelt. Daarbij kan nog worden opgemerkt dat, daar waar onverhoopt twijfel zou kunnen ontstaan aan de rechtsgeldigheid van een elektronisch proces-verbaal, dit de rechter er niet van behoeft te weerhouden om een dergelijk proces-verbaal te gebruiken als «een ander geschrift», in de zin van artikel 344, eerste lid, onder 5°, van het Wetboek van Strafvordering. De rechter is vrij daaraan de bewijskracht toe te kennen die hem verantwoord lijkt, met inachtneming van hetgeen in artikel 344 Sv is gesteld.

5. Aanvullende eisen voor het elektronisch proces-verbaal

In dit besluit worden, aanvullend op de regeling van de elektronische handtekening in het Burgerlijk Wetboek, specifieke eisen gesteld voor het gebruik van een elektronisch proces-verbaal in het strafproces. Deze eisen betreffen de volgende aspecten.

In de eerste plaats is vereist dat een elektronisch proces-verbaal wordt voorzien van een elektronische dagtekening en dat het wordt opgemaakt in een formaat dat voldoet aan het bij of krachtens de Archiefwet gestelde. Met behulp van de dagtekening wordt invulling gegeven aan het wettelijk vereiste dat het proces-verbaal is gedagtekend. Tevens dient de dagte-

kening om de geldigheid van het gehanteerde certificaat op het moment van de dagtekening, en daarmee de geldigheid van een elektronische handtekening, op een later tijdstip vast te kunnen stellen. De regels over het formaat zijn van belang voor de archivering van een elektronisch proces-verbaal.

In de tweede plaats worden eisen gesteld op het gebied van de bewaring van het elektronisch proces-verbaal en de elektronische handtekening, inclusief de dagtekening. Om aan zijn wettelijke verplichtingen te kunnen voldoen is een certificatiedienstverlener gehouden zelf de nodige gegevens te bewaren en te publiceren over de uitgifte van een gekwalificeerd certificaat (art. 2 besluit elektronische handtekeningen). In aanvulling op die verplichting moeten de in de bijlage (II) bij dit besluit opgenomen gegevens binnen de strafrechtsketen beschikbaar blijven zodat de geldigheid van het certificaat en de elektronische handtekening onweerlegbaar kunnen worden aangetoond, ook nadat de certificatiedienstverlener daarover geen informatie meer kan verschaffen.

In de derde plaats worden eisen gesteld over de verzending van een elektronisch proces-verbaal binnen de strafrechtsketen. Onderdeel daarvan vormen verplichtingen omtrent de validatie van het proces-verbaal nadat het ontvangen is van een persoon of instantie die het proces-verbaal verzonden heeft. Als de validatie uitwijst dat het elektronisch proces-verbaal is gewijzigd nadat dit met een elektronische handtekening is ondertekend dan is degene die het betreffende document heeft verzonden gehouden te voorzien in een elektronisch proces-verbaal dat voldoet aan de eisen van dit besluit.

Tenslotte worden regels gesteld over de beveiliging van het elektronisch proces-verbaal, de gegevens van het certificaat en de validatie.

6. Digitaal afschrift van een proces-verbaal

In dit besluit worden tevens regels gegeven over het digitaal afschrift van een proces-verbaal. Dit is een identieke weergave van een papieren proces-verbaal. Door middel van scannen wordt een papieren proces-verbaal omgezet in een elektronisch bestand. Dit kan worden onderscheiden van het kopiëren van een proces-verbaal, zodat een papieren afschrift van dat proces-verbaal wordt vervaardigd. In de jurisprudentie is het gebruik van een kopie van een proces-verbaal reeds langere tijd aanvaard. Reeds in 1948 is door de Hoge Raad geoordeeld dat een afschrift van een proces-verbaal, gewaarmerkt als eensluidend met het origineel, met het origineel gelijk staat (HR 25-05-1948, NJ 1948, 470). In 1978 heeft de Hoge Raad dit verruimd door te oordelen dat met het origineel van een proces-verbaal mag worden gelijkgesteld een voor «fotokopie cfm. origineel» gewaarmerkte fotokopie, ook indien die waarmerking niet is geschied door de verbalisant, maar door een andere, tot het opsporen van het ten laste gelegde strafbaar feit bevoegde, opsporingsambtenaar (HR 12-09-1978, NJ 1979, nr. 95). Later heeft het hoogste rechtscollege een niet gewaarmerkte fotokopie van een proces-verbaal aangemerkt als «een ander geschrift», in de zin van artikel 344, eerste lid, onder 5°, van het Wetboek van Strafvordering (HR 18-11-1980, NJ 1981, 134 en HR 10-03-1987, NJ 88, no. 25). Deze geschriften kunnen alleen voor het bewijs gelden in verband met de inhoud van andere bewijsmiddelen.

Inmiddels zijn bij het openbaar ministerie scanstraten ingericht waar papieren processen-verbaal langs elektronische weg worden omgezet in digitale afschriften. Dit is van groot belang voor een efficiënte bedrijfsvoering binnen de strafrechtsketen. Immers, indien het voor bepaalde

personen of organisaties binnen de strafrechtsketen (nog) niet mogelijk is te voorzien in een elektronisch proces-verbaal overeenkomstig de eisen van dit besluit, dan kan daarin alsnog worden voorzien door het papieren proces-verbaal om te zetten in een digitaal afschrift. Daarom worden in dit besluit tevens regels gegeven over het omzetten van een papieren proces-verbaal in een digitaal afschrift. Met behulp van een elektronische handtekening als waarmerk wordt bevestigd dat het digitaal afschrift een identieke weergave vormt van een papieren proces-verbaal. Een ambtenaar is bevoegd tot het plaatsen van een elektronische handtekening als waarmerk, dit is niet beperkt tot de ambtenaar die bevoegd is tot de opsporing van strafbare feiten. Het kan – anders dan tot nu toe in de jurisprudentie over de fotokopie – ook gaan om een ambtenaar die niet bevoegd is tot de opsporing van strafbare feiten. Deze ambtenaar moet door de verantwoordelijke formeel zijn aangewezen.

Voor de eisen aan een elektronisch proces-verbaal dat is verkregen door een papieren proces-verbaal om te zetten in een digitaal afschrift, wordt uitgegaan van dezelfde eisen als voor een langs elektronische weg opgemaakt proces-verbaal. Wel worden specifieke eisen gesteld aan het scanproces, zodat gewaarborgd is dat het digitaal afschrift een identieke weergave vormt van het papieren proces-verbaal.

Voor de kwaliteit van het digitaal afschrift is het van belang dat wordt gescand van het originele papieren proces-verbaal en dat de scan een juiste en volledige weergave is van het origineel. Verder moet het scanproces op zodanige wijze worden ingericht dat voldaan wordt aan de eisen, normen en standaarden die hiervoor binnen de overheid worden gehanteerd. Daarbij komt een belangrijke rol toe aan de regels voor de digitale vervanging van archiefbescheiden, op basis van de Archiefwet 1995 (art. 7 Archiefwet). Hiermee wordt gedoeld op het vervangen van een origineel document door een reproductie in elektronische vorm. Het originele document wordt gescand en omgezet in een elektronisch bestand waarna het elektronische document voortaan als het originele document geldt. Het oorspronkelijke document kan hierna worden vernietigd, behoudens uitzonderingen. De Beleidsregel digitale vervanging archiefbescheiden van de Minister van Onderwijs, Cultuur en Wetenschap, heeft betrekking op de verstrekking van een machtiging voor de vervanging van permanent te bewaren archiefbescheiden[1]. Hoewel dit laatste thans nog niet wordt nagestreefd in de strafrechtsketen, wordt voor de regels voor het scannen van papieren processen-verbaal binnen de strafrechtsketen nauw aangesloten bij de regeling van de Archiefwet 1995. Hierdoor is een zorgvuldig scanproces gewaarborgd. Deze regels zijn opgenomen in een bijlage (I) bij dit besluit. Aanvullend kunnen bij Ministeriële regeling nadere regels worden gegeven die dit verder uitwerken.

Als er aanwijzingen zijn dat een digitaal afschrift geen identieke weergave vormt van het papieren proces-verbaal dan is degene die het betreffende document heeft verzonden gehouden te voorzien in een elektronisch proces-verbaal dat voldoet aan de eisen van dit besluit.

Een proces-verbaal is van essentiële betekenis voor het bewijs in een strafzaak. Thans bestaat echter onvoldoende ervaring met het scannen van processtukken om bij voorbaat absolute zekerheid te kunnen geven over de mogelijkheid of wenselijkheid van vernietiging van het originele papieren proces-verbaal. Vanuit het oogpunt van de rechtszekerheid is het dan ook aangewezen om eerst de nodige ervaring op te doen met digitale afschriften van processen-verbaal, op basis van de regeling van dit besluit, om daarover een dergelijke mate van zekerheid te kunnen verkrijgen. Ingeval er in een voorkomend geval alsnog onzekerheid mocht bestaan dan kan altijd het originele papieren proces-verbaal worden

[1] Beleidsregel van de Minister van Onderwijs, Cultuur en Wetenschap van 22 januari 2008, nr. WJZ/2008/452 (8218), inzake de bevoegdheid tot het afgeven van een machtiging als bedoeld in artikel 7 van de Archiefwet 1995 ten behoee van routinematige digitalisering van archiefbescheiden (Beleidsregel digitale vervanging archiefbescheiden).

opgevraagd ter verificatie van het digitale afschrift. Voor alle zekerheid moeten de originele papieren processen-verbaal dus worden opgeslagen en bewaard, overeenkomstig de geldende regels. Niet uitgesloten is dat in de nabije toekomst, bijvoorbeeld in het kader van de wettelijke regeling van het elektronisch strafdossier, ook regels worden opgenomen over de digitale vervanging van processen-verbaal. Dan zal de praktijk van het «dubbel bewaren» van een proces-verbaal, van zowel het originele papieren proces-verbaal als het afschrift in elektronische vorm, tot het verleden kunnen gaan behoren.

7. Opslag en bewaring van een elektronisch proces-verbaal

De persoonsgegevens van een elektronisch proces-verbaal vallen onder de reikwijdte van de Wet politiegegevens (WPG) en van de Wet justitiële en strafvorderlijke gegevens (WJSG). De WPG is van toepassing op elk gegeven betreffende een geïdentificeerde of identificeerbare persoon dat in het kader van de uitoefening van de politietaak wordt verwerkt. De Wet justitiële en strafvorderlijke gegevens van toepassing op de persoonsgegevens die door het openbaar ministerie worden verwerkt.

Daarnaast is de Archiefwet (Aw) van toepassing omdat een proces-verbaal een archiefbescheid is in de zin van de Archiefwet.

Uitgangspunt van de WPG is dat politiegegevens worden vernietigd zodra zij niet langer noodzakelijk zijn voor de uitvoering van de politietaak. Voor de verschillende doelen binnen de politietaak, ten behoeve waarvan politiegegevens worden verwerkt, zijn maximale verwerkingstermijnen vastgesteld. Na verloop van de verwerkingstermijn moeten de gegevens worden verwijderd. Zo kunnen politiegegevens, die worden verwerkt ten behoeve van de uitvoering van de dagelijkse politietaak, worden verwerkt voor een periode van ten hoogste vijf jaar (art. 8, zesde lid, WPG). Voor een onderzoek in verband met de handhaving van de rechtsorde in een bepaald geval geldt dat de gegevens kunnen worden verwerkt zo lang zij nodig zijn voor het betreffende onderzoek (art. 9, vierde lid, WPG). Voor politiegegevens die inzicht geven in de betrokkenheid van personen bij bepaalde ernstige bedreigingen van de rechtsorde, waaronder de zogenaamde CIE-gegevens, geldt een verwerkingstermijn van ten hoogste vijf jaar (art. 10, zesde lid, WPG).

De verwijderde politiegegevens kunnen vervolgens gedurende een periode van vijf jaar worden bewaard met het oog op de afhandeling van klachten en de verantwoording van verrichtingen. Daarna worden de politiegegevens vernietigd. Van de vernietiging kan worden afgezien voorzover de waarde van de archiefbescheiden als bestanddeel van het cultureel erfgoed of voor historisch onderzoek zich daartegen verzet. De gegevens worden zo spoedig mogelijk overgebracht naar een archiefbewaarplaats. De Archiefwet 1995 is dan van toepassing (art. 14 WPG).

De korpsbeheerder is verplicht selectielijsten te maken waarin wordt aangegeven welke archiefbescheiden voor vernietiging in aanmerking komen en welke archiefbescheiden niet voor vernietiging in aanmerking komen zodat deze laatste categorie na 20 jaar naar een archiefbewaarplaats wordt overgebracht. In artikel 45 van de Politiewet is de grondslag neergelegd voor de zorg voor de archiefbescheiden. Dit heeft een verdere uitwerking gekregen in het Besluit beheer regionale politiekorpsen (Stb. 1994, 224). De regeling komt erop neer dat de gemeente is belast met het toezicht op de naleving van de Archiefwet 1995 voor de archiefbescheiden die bij de politie liggen. Het dagelijks bestuur van Politie Nederland heeft de zorg voor en het toezicht op de bewaring en het beheer van de archiefbescheiden van Politie Nederland (art. 8 Voorziening tot samenwerking Politie Nederland, Stcrt 2006, nr. 129).

Als een proces-verbaal wordt verzonden aan het openbaar ministerie, dan is de Wet justitiële en strafvorderlijke gegevens van toepassing op de persoonsgegevens die in het proces-verbaal zijn opgenomen en die het openbaar ministerie in een strafdossier of langs geautomatiseerde weg verwerkt (art. 1, onderdeel b, WJSG). De hoofdregel is dat de strafvorderlijke gegevens met betrekking tot misdrijven dertig jaar na de onherroepelijke afdoening van de strafzaak worden verwijderd. Voor overtredingen geldt een termijn van vijf jaar (art. 39d WJSG). In beide gevallen wordt de termijn verlengd afhankelijk van de opgelegde straf. De WJSG regelt niets over vernietiging van gegevens. Dit wordt dus in zijn geheel geregeld door de Archiefwet 1995. Evenals bij de processen verbaal bij de politie moeten bij het openbaar ministerie selectielijsten worden gemaakt waarin de Minister van Justitie aangeeft welke bescheiden moeten worden bewaard en welke moeten worden vernietigd. Dit is geregeld in de Vaststelling selectielijst beleidsterrein rechterlijke macht vanaf 1950 (Stcrt 2003, 11). Daarin is bepaald dat processen verbaal in kantongerechtzaken na zeven jaar worden vernietigd en in rechtbankzaken na tien jaar of, ingeval het betreft een niet onherroepelijke zaak, na achttien jaar. In het besluit zijn de afwegingen weergegeven op basis waarvan deze vernietigingstermijnen zijn gebaseerd.

In de Archiefregeling, die op 1 april 2010 in werking is getreden, zijn bijzondere voorschriften opgenomen voor te bewaren digitale archiefbescheiden[1]. Deze voorschriften hebben betrekking op de functionele eisen, de koppeling van metagegevens aan digitale archiefbescheiden en algemene eisen aan opslagformaten (artikelen 21 tot en met 26). Het bestandsformaat moet voldoen aan een open standaard. De hierin opgenomen elementen met betrekking tot de elektronische handtekening zijn echter niet voldoende toegesneden op het gebruik in strafrechtelijke procedures.

8. Financiële paragraaf

Om elektronisch opgemaakte processen-verbaal, voorzien van een elektronische hand- en dagtekening te kunnen aanleveren, is het nodig de proceshandelingen te ondersteunen in de primaire processystemen van politie (Basisvoorziening Handhaving, Basisvoorziening Opsporing, Transactiemode) en van de bijzondere opsporingdsdiensten. Het gaat hierbij om de implementatie van nieuwe systemen die veel extra inzet van capaciteit bij politie vergt. Het zal naar verwachting daarom nog enkele jaren duren voordat de politie en de bijzondere opsporingsdiensten op grote schaal elektronisch ondertekende processen-verbaal bij het openbaar ministerie gaan aanleveren.

In afwachting van bovengenoemde aanpassing van de bestaande processen en systemen bij de politie en de bijzondere opsporingsdiensten zal het Openbaar Ministerie gebruik maken van de mogelijkheid die dit besluit biedt om digitale afschriften te maken van de ingezonden papieren processen-verbaal. Het Openbaar Ministerie heeft daartoe bij alle parketten een scanstraat ingericht. Voor de omzetting van de grote documentenstroom is het Openbaar Ministerie voornemens gebruik te gaan maken van de diensten die de Justitiële Informatiedienst als centrale postbus en scanfaciliteit wil en kan leveren. Beide justitie-organisaties hebben de intentie uitgesproken te komen tot een contract dat erin voorziet dat de Justitiële Informatiedienst van nagenoeg alle bij de parketten binnenkomende processen-verbaal en overige schriftelijke bescheiden van het strafdossier, elektronische afschriften maakt, conform de voorschriften in artikel 4. Deze afschriften zullen worden voorzien van een elektronische handtekening als waarmerk. De Justitiële Informatiedienst beschikt al over een geavanceerde scanfaciliteit.[2] De capaciteit

[1] Regeling van de Minister van Onderwijs, Cultuur en Wetenschap van 15 december 2009, nr. WJZ/178205 (8189), met betrekking tot de duurzaamheid en de geordende en toegankelijke staat van archiefbescheiden en de bouw en inrichting van archiefruimten en archiefbewaarplaatsen (Archiefregeling).

[2] De Justitiële Informatiedienst heeft inmiddels ruime ervaring met het omzetten van papieren documenten in digitale documenten met het oog op digitale archivering in het Centrale Digitale Depot (CDD+) Onlangs heeft de Justitiële Informatiedienst een contract gesloten met de Immigratie en Naturalisatiedienst om alle papieren processtukken om te zetten in en te vervangen door digitale stukken.

hiervan zal moeten worden uitgebreid. Aan enkele tientallen medewerkers bij de Justitiële Informatiedienst belast met het maken van digitale afschriften, zullen certificaten moeten worden uitgegeven. De budgettaire gevolgen zullen door het Openbaar Ministerie binnen de begroting worden opgelost.

Het besluit zal voor de politie en de bijzondere opsporingsdiensten pas budgettaire gevolgen hebben op het moment dat besloten wordt processen-verbaal op elektronische wijze, voorzien van een elektronische handtekening, te leveren aan het Openbaar Ministerie. Dan zullen kosten ontstaan als gevolg van daarvoor noodzakelijke aanpassingen aan de processen, primaire systemen, aanschaf van randapparatuur (zoals kaartlezers) en aanvullende organisatorische en ICT-voorzieningen. Deze voorzieningen zullen eenmalige en structurele beheerkosten met zich brengen. Ook zullen alsdan structurele kosten zijn gemoeid met de uitgifte van certificaten. Hoewel dit wenselijk is, kan thans nog niet worden voorzien of deze certificaten zullen worden ondergebracht in de Rijkspas of anderszins in een Politietoegangspas. Afhankelijk van de keuze die wordt gemaakt zullen kosten hoger of lager uitvallen. De kosten gemoeid met de uitgifte van tekencertificaten onder de in totaal 25.000 politieambtenaren die Nederland telt, bedragen naar verwachting hooguit 3 miljoen euro per jaar (€ 120 per tekencertificaat). Met een procedure waarin de tekencertificaten worden bijgeplaatst op een pas voor meerdere doeleinden, zullen de kosten aanzienlijk lager kunnen uitvallen. Nu landelijke invoering van de elektronische handtekening ten behoeve van het elektronische proces-verbaal pas op termijn zal kunnen plaatsvinden, heeft dit besluit geen onmiddellijke budgettaire gevolgen voor de politie en de bijzondere opsporingsdiensten.

Voor de aanvullende bewaring van gegevens over de geldigheid van de elektronische handtekening (artikel 3) zijn systemen op de markt beschikbaar. De kosten daarvan kunnen worden geschat op € 30.000.– voor een compleet systeem dat door meerdere partijen kan worden gebruikt.

Om te voorzien in een duurzame opslag en valideerbaarheid van het elektronische proces-verbaal en andere bescheiden van het strafdossier, wordt de Waarmerk- Teken en Validatieservice (WTV-service) en een veilig depot (CCD+) ingericht. In de toelichting bij artikel 5, tweede lid, wordt hier nader op in gegaan. De beheerkosten hiervan worden geschat op een kleine half miljoen euro per jaar.

Een eerste raming van de materiele opbrengsten van de digitalisering van het strafdossier is twee jaar geleden gemaakt in een tweetal business cases, uitgevoerd in het kader van het project Digitaal Procesdossier Loopzaken in Rotterdam en Amsterdam[1]. In de business cases wordt een besparing begroot van meer dan € 340.000.– per jaar respectievelijk € 737.000.– per jaar. Daarbij zij opgemerkt dat de business case Amsterdam een scenario doorrekent waarbij nog geen sprake is van volledige digitale overdracht en waarbij nog steeds transport-, papier- en kopieerkosten worden gemaakt. Een extrapolatie naar landelijk niveau van de in de beide business cases berekende jaarlijkse opbrengsten, leert dat de digitalisering uiteindelijk 4 tot 7 miljoen euro aan vrijkomende middelen per jaar kan opleveren.[2]

De kwalitatieve opbrengsten die het openbaar ministerie en de zittende magistratuur op termijn voorzien zijn aanzienlijk. Deze opbrengsten zijn:
een beter beheer van de strafdossiers en het niet meer hoeven verplaatsen van papier, waardoor minder fouten worden gemaakt en er minder uitval zal zijn;

[1] Business Case Digitaal Procesdossier Rotterdam, Barbera Krop, 15 april 2005. *Nulmeting* Digitaal Procesdossier Politie en Parket Amsterdam, Capgemini NV, Utrecht, 8 december 2006.

[2] Voor beide politiekorpsen geldt dat zij elk ongeveer 10% van de landelijke korpssterkte representeren. De extrapolatie behelst een vermenigvuldiging van de lokaal in beeld gebrachte opbrengsten met factor 10.

geen tijdverlies meer vanwege verzenden, verplaatsen, ordenen, samenstellen en complementeren van strafdossiers, waardoor kortere doorlooptijden kunnen worden gerealiseerd;

«real time» beschikbaarheid van (onderdelen van) het strafdossier voor daartoe bevoegde functionarissen en procesdeelnemers, waardoor onder meer de rechter-commissaris beter aan zijn taakopdracht toekomt, strafzaken beter voorbereid op zitting worden gebracht, procesdeelnemers meer gelijkelijk geïnformeerd zullen zijn en er minder aanleiding zal bestaan tot schorsing of onderbreking van de strafzaak;

verbetering van de informatievoorziening rondom de afloop van zaken.

De totale budgettaire gevolgen voor de politie zullen nader in beeld gebracht worden met behulp van een impactanalyse waarin ook andere (lopende) pilots dan de genoemde in Rotterdam en Amsterdam betrokken worden. Het doel van deze impactanalyse is, te bepalen op welke wijze en onder welke condities invoering van de elektronische handtekening ten behoeve van het elektronisch proces-verbaal het best kan plaatsvinden. De kosten van de impactanalyse worden gedragen door de ministeries van Binnenlandse Zaken en Koninkrijksrelaties en van Justitie gezamelijk.

Een compleet overzicht van de kosten die zijn verbonden aan het gebruik van het elektronisch proces-verbaal door de ambtenaren van de bijzondere opsporingsdiensten is in dit stadium nog niet te geven. De inschatting is dat het gebruik van de elektronische handtekening jaarlijks tussen de € 130.– en € 150.– euro per geautoriseerde medewerker zal bedragen (autorisatie, certificatie, beheer). Kosten voor archivering zijn op dit moment niet te geven. Deze indicatie betekent voor de bijzondere opsporingsdiensten totaal, uitgaande van het aantal van 1500 geautoriseerde medewerkers, € 150.000.– tot € 200.000.– aan jaarlijkse kosten.

De totale invoering van het elektronisch proces-verbaal wordt voor de overheid als geheel vooralsnog als budgettair neutraal ingeschat. Het vergroten van de efficiency in de strafrechtelijke procedure zal besparingen opleveren. Daar staat tegenover dat kosten dienen te worden gemaakt om de invoering van het elektronische proces-verbaal mogelijk te maken. Op basis van de impactanalyse en een aanvullende pilot zullen de totale kosten en baten voor de overheid in beeld gebracht worden en evenredig verdeeld worden over de beleidsverantwoordelijke departementen. Op basis van de uitkomsten van de pilots zullen tussen de betrokken departementen nadere afspraken worden gemaakt over de verdeling van de kosten rond de invoering van het elektronische proces-verbaal.

9. De uitgebrachte adviezen

Over het ontwerpbesluit is advies uitgebracht door het College van procureurs-generaal, de Raad voor de rechtspraak, de Nederlandse Vereniging voor Rechtspraak, de Raad van Korpschefs i.o. en de Nederlandse Orde van Advocaten.

Het College van procureurs-generaal stelt vast dat in het conceptbesluit elektronisch proces-verbaal terecht grote waarde wordt gehecht aan het waarborgen van de authenticiteit en integriteit van het door een opsporingsambtenaar opgemaakte proces-verbaal. De strenge eisen aan het elektronische proces-verbaal zijn volgens het College verstandig en begrijpelijk, evenals de voorzichtigheid rond de vernietiging van originele papieren processen-verbaal. Algemeen gesproken stemt het College in met de in het conceptbesluit gevolgde voorzichtige benadering. Wel betreurt het College dat de reikwijdte van de wet en het besluit niet iets ruimer is gemaakt. Zoals in het algemeen deel van de memorie van

toelichting aan de orde is gekomen, wordt deze beperking ingegeven door de reikwijdte van artikel 153 van het Wetboek van Strafvordering. Mede in het licht van de modernisering van het Wetboek van Strafvordering zal de wenselijkheid en mogelijkheid van een meer omvattende regeling van het elektronisch verkeer in het strafprocesrecht in de nabije toekomst nader worden bezien.

Het College merkt verder op dat het hier om een tamelijk technische materie gaat, waarvan het begrip verbeterd zou worden als in de nota van toelichting een passage zou worden opgenomen waarin concreet en feitelijk worden aangegeven welke handelingen verricht moeten worden bij het opmaken en verzenden van een elektronisch proces-verbaal. Daarbij kan wellicht ook worden ingegaan op de rol van de WTV-service. Aan dit advies is gevolg gegeven, in die zin dat de door het College aangehaalde aspecten op verschillende plaatsen in de toelichting zijn verhelderd.

Tenslotte heeft het College een artikelsgewijs commentaar ingebracht. De opmerkingen over artikel 1, artikel 2, artikel 4, eerste lid en artikel 6 zijn overgenomen. De omschrijving van het begrip «digitaal afschrift», in artikel 1, onderdeel a, is aangepast. Het woord authenticatie, in artikel 1, onderdeel d, is vervangen door het woord «authentificatie». In artikel 2, tweede lid, zijn de woorden «van een wettelijk opgemaakt schriftelijk proces-verbaal» geschrapt. In artikel 4, eerste lid, zijn de woorden «onder meer» geschrapt. De in dat lid genoemde voorschriften zijn opgenomen in een Bijlage (I) bij dit besluit. Naar aanleiding van de opmerking over artikel 4, tweede lid, is de nota van toelichting aangevuld.

De Raad voor de rechtspraak wijst op de aanzienlijke voordelen van digitalisering van papieren strafdossiers. Het Openbaar Ministerie en de Rechtspraak willen de vervanging van papieren dossiers door digitale dossiers bevorderen. Zij doen dat in de verwachting dat ook de politie processen-verbaal van opsporingsambtenaren elektronisch zal opmaken en langs elektronische weg aan de parketten zal zenden. Het ontwerpbesluit voorziet in belangrijke mate in de voor deze ontwikkeling onmisbare regelgeving. De Raad steunt deze ontwikkeling en onderschrijft dat in het ontwerpbesluit gekozen is voor de gekwalificeerde elektronische handtekening; de betrouwbaarheid van het elektronische proces-verbaal dient boven iedere twijfel verheven te zijn. De Raad attendeert erop dat de voorgestelde regeling slechts ziet op processen-verbaal van opsporingsambtenaren. De regeling van de elektronische handtekening door één of meer opsporingsambtenaren roept de vraag op hoe om te gaan met de ondertekening van hun verklaringen door verdachten of getuigen. In de praktijk bestaat hieraan behoefte. De Raad attendeert op de noodzaak om aan dit aspect aandacht te schenken en geeft als oplossing de mogelijkheid dat een scan van een door een verdachte of getuige op papier ondertekende verklaring als bijlage wordt gevoegd bij het elektronische proces-verbaal. Naar aanleiding van dit advies kan worden opgemerkt dat een regeling van de elektronische handtekening van verdachten of getuigen, zoals ook de Raad zelf opmerkt, buiten het bestek van dit besluit valt. Gedacht kan worden aan de ondertekening van een elektronisch proces-verbaal met behulp van een digitale pen, een vingerafdruk of een digitale scan van een op papier ondertekende verklaring. Niet uitgesloten is dat dergelijke oplossingen in de rechtspraktijk worden aanvaard, zonder dat dit expliciet geregeld is. Daarnaast zal dit punt kunnen worden betrokken in de wettelijke regeling van het elektronisch strafdossier.

Verder wijst de Raad erop dat in de nota van toelichting informatie ontbreekt over de mogelijkheid om een elektronisch proces-verbaal door één of meerdere opsporingsambtenaren te ondertekenen. Ook ontbreekt een beschrijving van de situatie waarin verbalisanten «anoniem» relateren, in een dergelijk geval wordt de verbalisant aangeduid met een

codenaam. De vraag rijst of het ontwerpbesluit in de mogelijkheid voorziet om een elektronisch proces-verbaal door meerdere verbalisanten en ook anoniem te ondertekenen door middel van een elektronische handtekening. Mede naar aanleiding van het advies van de Raad van Korpschefs is in artikel 3 de ruimte geboden voor het gebruik van een pseudoniem door de ondertekenaar van een elektronisch proces-verbaal. Tevens is in de nota van toelichting verduidelijkt dat één of meerdere verbalisanten een elektronisch proces-verbaal kunnen ondertekenen.

De Raad wijst er op dat de verwijzing naar de Beleidsregel digitale vervanging archiefbescheiden, in artikel 4 van het ontwerpbesluit, ertoe kan leiden dat wijzigingen in de beleidsregel worden doorgevoerd zonder dat de rechtspraak daarbij betrokken is. Deze wijzigingen kunnen echter consequenties hebben voor de inrichting van het scanproces. Naar aanleiding van dit advies zijn de relevante elementen van de Beleidsregel digitale vervanging archiefbescheiden opgenomen in een bijlage (I) bij het ontwerpbesluit.

Tevens merkt de Raad op dat in de nota van toelichting wordt aangegeven dat de originele, papieren versie van een gescand proces-verbaal moet worden bewaard, Een duidelijke verplichting daartoe ontbreekt echter in het ontwerpbesluit. De Archiefwet 1995 gaat uit van vernietiging van een papieren origineel, waarbij de scan het papieren origineel vervangt. Er is dan sprake van substitutie, zodat de in het ontwerpbesluit gehanteerde term «afschrift» volgens de Raad minder juist gekozen is. In reactie op dit advies moet worden opgemerkt dat het ontwerpbesluit er vooralsnog inderdaad vanuit gaat dat de originele, gescande versie van een papieren proces-verbaal na het scannen bewaard blijft. De Archiefwet 1995 voorziet uitsluitend in het vernietiging van een papieren proces-verbaal na vervanging. Er is in de voorgestelde regeling echter geen sprake van digitale vervanging in de zin van de Archiefwet 1995, reden waarom gekozen is voor het gebruik van de term «afschrift». Op basis van de ervaringen met het scannen van papieren processen-verbaal zal in de nabije toekomst kunnen worden overgestapt op digitale vervanging, bijvoorbeeld in het kader van de wettelijke regeling van het elektronisch strafdossier.

Voorts dringt de Raad erop aan de eisen zo in te richten dat het elektronisch proces-verbaal voor een ieder toegankelijk is (ook met spraakcomputer of brailleapparatuur), en dat de inhoud daarvan eenvoudig doorzoekbaar en herbruikbaar is. In reactie op dit advies kan worden opgemerkt dat het ontwerpbesluit voorschrijft dat een elektronisch proces-verbaal wordt opgesteld in een documentformaat dat voldoet aan het bij of krachtens de Archiefwet 1995 bepaalde. Hiermee is gewaarborgd dat gebruik wordt gemaakt van gangbare formaten zoals de PDF/A1-standaard en XML. De keuze voor een duurzaam gangbaar formaat garandeert dat de tekst toegankelijk is en dat voldoende programmatuur beschikbaar is voor het lezen en doorzoeken van de tekst.

Voor wat betreft de werklast voorziet de Raad geen significante gevolgen voor de gerechten. Wel moet met aanzienlijke uitvoeringsproblemen rekening worden gehouden als het ontwerpbesluit in werking treedt op een moment dat de rechtspraak daarop nog onvoldoende is voorbereid en ingesteld. Deze problemen moeten worden geïnventariseerd en overdacht. Daarbij suggereert de Raad uitdrukkelijk te regelen dat een geprint elektronisch proces-verbaal, dat voor «kopie conform» is getekend door een opsporingsambtenaar, gelijk gesteld moet worden met het digitale origineel. Deze voorziening biedt de rechtspraak de mogelijkheid om in voorkomende gevallen gedurende de implementatiefase te blijven werken met een papieren dossier. Dit advies is niet overgenomen omdat dit besluit primair beoogt te voorzien in regels voor het elektronisch proces-verbaal, zodat dit dezelfde bewijskracht toekomt als een papieren proces-verbaal dat door een opsporingsambtenaar is gedagtekend en ondertekend. Er is geen wettelijke basis voor een regeling

van het gebruik van een papieren afschrift van een elektronisch proces-verbaal, artikel 153 van het Wetboek van Strafvordering biedt daarvoor geen rechtsgrondslag. Ook is een dergelijke regeling minder goed verenigbaar met de beleidsmatige keuze voor een overwijlde invoering van het elektronisch proces-verbaal binnen de strafrechtsketen. Het staat de rechterlijke macht overigens vrij om in voorkomende gevallen een papieren uitdraai van een elektronisch proces-verbaal te gebruiken. Desgewenst kan daarbij gebruik worden gemaakt van een handtekening voor «kopie conform», zoals deze op grond van de jurisprudentie inmiddels is aanvaard voor een kopie van een papieren proces-verbaal.

Tenslotte heeft de Raad een aantal redactionele opmerkingen ingebracht. Deze zijn deels overgenomen, dit is in de nota van toelichting verwerkt.

De Nederlandse Vereniging voor rechtspraak (NVvR) onderschrijft het besluit voor zover de vereniging de technische onderdelen kan beoordelen, en plaatst enkele kanttekeningen van voornamelijk praktische aard. De NVvR vraagt aandacht voor de problemen die de praktijk reeds ondervindt met de beveiliging van bestanden. Zij is van mening dat grootscheepse wijzigingen pas doorgevoerd zouden mogen worden indien de verwerkingsapparatuur geschikt en in voldoende mate beschikbaar is. Daarbij vraagt de NVvR aandacht voor de eisen die de Arbeidsomstandighedenwet stelt. Voorts zou de NVvR graag zien dat het mogelijk blijft dat verschillende verbalisanten één proces-verbaal kunnen opmaken. Naar aanleiding van dit advies moet worden opgemerkt dat het ontwerpbesluit geen specifieke eisen voor de beveiliging van documenten en informatiesystemen bevat, aangesloten wordt bij de eisen, maatregelen en voorschriften die binnen de betreffende organisatie gebruikelijk zijn. Uitgangspunt is het informatiebeveiligingsbeleid van de organisatie en de daarbij passende toegangsbeveiliging. Voorzover de Arbeidsomstandighedenwet eisen stelt rond op het werken met beeldschermen, dan zullen die eisen onverkort van toepassing zijn. De werkgever is verantwoordelijk voor de organisatie en inrichting van digitale werkplekken conform de richtlijnen van de Arbeidsomstandighedenwet, meer specifiek de artikelen 5.7 tot en met 5.12 van het Arbeidsomstandighedenbesluit. Op dit punt vormt het ontwerpbesluit geen uitzondering. Mede naar aanleiding van het advies van de Raad voor de rechtspraak is in de nota van toelichting verduidelijkt dat één of meerdere verbalisanten een elektronisch proces-verbaal kunnen ondertekenen.

De NVvR mist de andere betrokkenen in het strafproces naast de politie, het openbaar ministerie en de rechters, zoals advocaten, reclassering en slachtoffers, en zou graag zien dat in het besluit, alsook in de nota van toelichting, aandacht wordt besteed aan deze betrokkenen. Zoals in de nota van toelichting is opgemerkt, geeft het ontwerpbesluit regels voor een elektronisch proces-verbaal van een opsporingsambtenaar, dat wordt opgesteld op grond van artikel 153 van het Wetboek van Strafvordering. Dit kan ook worden aangeduid als een proces-verbaal van bevindingen. De wenselijkheid en mogelijkheid van een meer omvattende regeling van het elektronisch verkeer in het strafprocesrecht zal nader worden bezien, zonodig in het kader van de modernisering van het Wetboek van Strafvordering.

Verder acht de NVvR de normadressaat van het voorgestelde artikel 6 niet duidelijk, noch welke sanctie er gesteld wordt op niet naleving van dit artikel. Naar aanleiding van dit advies is de tekst van dit artikel verhelderd. Indien de in dit artikel neergelegde verplichtingen niet worden nageleefd is er geen sprake van een elektronisch proces-verbaal dat aan de wettelijke eisen voldoet. In bepaalde gevallen is de verantwoordelijke, namens wie het elektronisch proces-verbaal is verzonden, gehouden om in een proces-verbaal te voorzien dat wel aan de eisen voldoet. Als dat niet mogelijk is of als er sprake is van andere tekortkomingen, dan is het

aan de rechter in een strafzaak om de rechtsgeldigheid van het proces-verbaal te beoordelen.

Tevens is de NVvR bezorgd of er voldoende rekening is gehouden met de extra werklast voor de rechterlijke macht en verzoekt om beschikbaarstelling van voldoende middelen voor opleiding, automatisering, aanschaf van apparatuur en dergelijke. Met het oog op deze vragen is het van belang dat de komende periode pilots worden gedaan. Zoals in paragraaf 8 is vermeld, kan na inwerkingtreding van dit besluit kleinschalig en in ketenverband worden gestart met de pilots, dit ter ondersteuning van de besluitvorming over tempo en wijze van definitieve implementatie. Wat betreft het openbaar ministerie vallen de kosten die gemaakt worden voor de invoering van het elektronische proces-verbaal binnen het bestek van de ontwikkel- en invoeringskosten van GPS. Binnen dat bestel is reeds rekening gehouden met de kosten. Het betreffen kosten die voor de baten uitgaan. Wat betreft de Rechtspraak kan in het kader van de komende kostprijsonderhandelingen worden bezien in hoeverre een compensatie noodzakelijk is van de extra kosten voor opleiding, automatisering en apparatuur en mogelijk ook het verlies aan inkomsten ingeval het openbaar ministerie in de aanloopperiode minder zaken zullen aanleveren.

Voorts wijst de NVvR erop dat het controleren van de gescande documenten op leesbaarheid en volledigheid tot extra werk zal leiden. De vraag die dit oproept is in hoeverre de huidige praktijk waarbij van het op papier gestelde originele proces-verbaal een gewaarmerkte kopie wordt gemaakt zou kunnen afwijken van en mogelijk minder arbeidsintensief zou kunnen zijn dan de beoogde praktijk waarbij van het op papier gestelde originele proces-verbaal een gewaarmerkt digitaal afschrift wordt gemaakt. In beide gevallen is de betekenis van de handtekening als waarmerk dat degene die heeft getekend ervoor instaat dat het afschrift een identieke weergave vormt van het origineel. De voorschriften zoals opgenomen in Bijlage I waarborgen een betere leesbaarheid en volledigheid, wat op termijn juist zal leiden tot minder (herstel)werk.

Tenslotte heeft de NVvR een aantal opmerkingen van juridisch-technische aard ingebracht. Deze zijn deels overgenomen, dit is in de nota van toelichting verwerkt.

De Raad van Korpschefs i.o. (RKC) is voorstander van de kwaliteitsverbeteringen en van efficiencymaatregelen, die met het elektronische proces-verbaal mogelijk zijn. Vooral het terug kunnen brengen van administratieve lasten spreekt de Raad van Korpschefs zeer aan. De Raad is echter bezorgd dat het ontwerpbesluit ertoe zal leiden dat de digitalisering van het proces-verbaal complex en duur wordt. Ook wordt er volgens de Raad verbinding gelegd met ontwikkelingen die nu nog niet bruikbaar zijn.

Vanuit het perspectief van de organisatie bepleit de Raad een stevige impactanalyse in enkele korpsen. Daarbij zal specifiek onderzocht moeten worden welke inspanningen vereist zijn voor het landelijke aanpassen en standaardiseren van de werkprocessen. Op basis van de uitkomsten kan dan kleinschalig en in ketenverband worden gestart met pilots waarin ervaringen kunnen worden opgedaan. Dit ter ondersteuning van de besluitvorming over tempo en wijze van definitieve implementatie.

Vanuit het perspectief van de ICT relateert het ontwerpbesluit de oplossing aan diverse overheidsontwikkelingen als PKIoverheid, Rijkspas en de elektronische Nederlandse identiteitskaart (eNIK). De Raad signaleert dat op dit moment geen overheidsbrede faciliteiten worden geboden waarmee invulling kan worden gegeven aan de in het conceptbesluit opgenomen eisen en adviseert de eis van de gekwalificeerde handtekening te vervangen die door van de geavanceerde handtekening. Volgens de raad kan het vereiste kwaliteitsniveau gehaald worden door de

gekwalificeerde handtekening te combineren met aanvullende afspraken of procedures.

Op basis van eerder opgedane ervaringen herkent de RKC het financiële beeld niet. De werkelijke kosten zullen vele malen hoger zijn. De Raad bepleit voor een beperking van de eisen aan de handtekening zelf en in het ontwerpbesluit ruimte te creëren voor een gefaseerde groei van papier naar digitaal via enerzijds technologie en anderzijds procesafspraken en waarborgen.

Naar aanleiding van het advies van de Raad is in de toelichting de beschrijving van de overheidsontwikkelingen met betrekking tot onder andere de Rijkspas aangepast. In reactie op dit advies kan daarnaast het volgende worden opgemerkt. Gedurende de afgelopen jaren is intensief overlegd over de invoering van het elektronische proces-verbaal in de strafrechtsketen. In de jaren 2006 en 2007 is een speciaal programma ingericht (ePV) waaraan is deelgenomen door vertegenwoordigers van de politie en het openbaar ministerie. In 2008 is, samen met vertegenwoordigers van de Nederlandse politie een impactanalyse uitgevoerd voor de elektronische handtekening. In paragraaf 8 is hierop ingegaan. Inmiddels zijn met vertegenwoordigers van de politie afspraken gemaakt over een brede impactanalyse, aan de hand van een businesscase, die tevens betrekking zal hebben op de inhoud van het ontwerpbesluit. De impactanalyse heeft betrekking op de invoering van het elektronisch dossier in de strafrechtsketen. Het elektronisch proces-verbaal vormt daarvan een belangrijk onderdeel. In dit kader zal ook aandacht worden geschonken aan de «spin off» van een dergelijk dossier voor de ketenpartners, zoals de verzending van afloopberichten en de verspreiding van dossierstukken. Naar verwachting zal de impactanalyse voor het eind van dit jaar worden afgerond, waarna nadere besluitvorming zal plaatsvinden in (nauw overleg met) de beraden. De resultaten van de impactanalyse kunnen aanleiding geven tot bijsturing van de werkprocessen, dit behoeft echter niet in de weg te staan aan de verdere procedure voor de invoering van het ontwerpbesluit.

In het algemeen deel van de nota van toelichting is de keuze voor een gekwalificeerde elektronische handtekening toegelicht. Hiermee wordt gekozen voor het hoogste niveau van betrouwbaarheid van een elektronische handtekening. Gelet op de functie van een proces-verbaal van een opsporingsambtenaar als bewijsmiddel in het strafproces is dit een logische keuze, die wordt ondersteund door de Raad voor de rechtspraak (en het Openbaar Ministerie). De gekwalificeerde elektronische handtekening voorkomt het bezwaar dat de authenticiteit en integriteit van het proces-verbaal in het geding zou kunnen zijn en dat degene die het proces-verbaal heeft opgemaakt kan worden geconfronteerd met de bewijslast daartoe. Daarnaast zijn er geen uniforme normen voor de invulling van een geavanceerde handtekening op basis waarvan vooraf vast staat dat deze voldoende betrouwbaar is. Dit was destijds een belangrijke overweging om, met de Wet elektronische handtekeningen, normen te stellen rond gekwalificeerde certificaten en het veilig middel. De suggestie van de Raad, om te eisen dat een oplossing vergelijkbare garanties geeft qua authenticiteit, integriteit en vergelijkbaarheid, biedt geen concrete aanknopingspunten voor een systeem dat binnen de strafrechtsketen breed wordt gedragen. Uniforme kwaliteitseisen binnen de strafrechtsketen zijn essentieel voor een goede toepassing van de elektronische handtekening door de ketenpartners.

In de financiële paragraaf zijn de kosten die zijn verbonden aan de invoering van de elektronische handtekening geraamd. De kosten die zijn gemoeid met een grootschalige uitgifte van tekencertificaten onder de in totaal 25.000 politieambtenaren zullen naar verwachting 3 miljoen euro per jaar bedragen. Daartegenover staan besparingen die op de lange termijn hoger zullen zijn dan de kosten. In het advies van de Raad wordt

geen nadere onderbouwing gegeven voor de opmerking dat de werkelijke kosten vele malen hoger zullen zijn dan geschetst in de nota van toelichting. De kosten zullen eerder lager kunnen zijn omdat de politie gebruik zal kunnen maken van de brede aanbesteding van toegangspassen. Tevens wordt door het Ministerie van Justitie de mogelijkheid onderzocht van een eigen geaccrediteerde certificatiedienstverlening, die voldoet aan de eisen van dit besluit.

Samenvattend adviseert de Raad het elektronisch proces-verbaal in pilotvorm uit te testen. Aan dit advies wordt tegemoetgekomen. Zoals in paragraaf 8 is beschreven, kunnen na inwerkingtreding van het besluit ketenbrede pilots worden gestart ten behoeve van de besluitvorming over het tempo en de wijze van implementatie.

Tenslotte heeft de Raad een artikelsgewijs commentaar ingebracht. De opmerkingen van dit commentaar zijn deels overgenomen, dit is in de nota van toelichting verwerkt.

De Nederlandse Orde van Advocaten (NOvA) geeft aan niet te beschikken over de deskundigheid om te beoordelen of de in het conceptbesluit opgenomen vereisten voldoende zijn om te verzekeren dat de authenticiteit en integriteit van het proces-verbaal afdoende gewaarborgd zijn. Daartoe zouden gekwalificeerde EDP-auditors het ontwerpbesluit moeten beoordelen. De NOvA acht het van belang dat er een onafhankelijke en onpartijdige beoordeling van de betrouwbaarheid en beveiliging van de informatiesystemen en de technische infrastructuur plaatsvindt en dringt erop aan dat die alsnog zal plaatsvinden. In reactie op dit advies moet worden opgemerkt dat de betrouwbaarheid en beveiliging van een gekwalificeerde handtekening boven iedere twijfel moet zijn verheven. De certificatiedienstverleners die gekwalificeerde certificaten afgeven zijn verplicht aan de toezichthouder OPTA informatie te verstrekken waaruit blijkt dat de dienstverlener aan de wettelijke eisen voldoet. Voorts wordt jaarlijks door de toezichthouder gevraagd om wijzigingen in de informatie door te geven en relevante documenten toe te sturen. Op basis van die informatie beoordeelt de toezichthouder of de certificatiedienstverlener aan de wettelijke eisen blijft voldoen. Daarnaast wordt gebruik gemaakt van vrijwillige accreditatiemechanismen. In de memorie van toelichting bij de Telecommunicatienet is hier nader op ingegaan (Kamerstukken II, 2000/01, 27 743, nr. 3, blz. 22/23). Gelet op de huidige waarborgen rond de afgifte van gekwalificeerde certificaten voor elektronische handtekeningen lijken extra audits weinig opportuun. Wel zal intensief en zorgvuldig moeten worden overlegd met de ketenpartners om ervoor te zorgen dat de invoering van de elektronische handtekening in de strafrechtsketen soepel verloopt. Hieraan zal de nodige aandacht worden geschonken.

Voor wat betreft het vereiste van de gekwalificeerde handtekening acht de Orde het werken met pincodes en certificaten niet voldoende, nu deze naar de mening van de Orde gemakkelijk kunnen worden doorgegeven. De NOvA dringt aan op het gebruik van biometrie om optimaal te verzekeren dat degenen die het proces-verbaal opmaakt dit ook ondertekent. In reactie op dit advies kan worden opgemerkt dat een gekwalificeerde handtekening de authenticiteit en integriteit van een elektronisch proces-verbaal afdoende waarborgt. De ondertekenaar van een elektronisch proces-verbaal heeft een private sleutel nodig, die op een veilig middel is geplaatst en waarbij uitsluitend toegang voor gebruik mogelijk is met behulp van een pincode. Het gebruik van een vingerafdruk behoort tot de mogelijkheden, maar is niet essentieel voor het waarborgen van de authenticiteit van een elektronisch proces-verbaal.

Voor wat betreft het scannen van papieren processen-verbaal is de NOvA is van oordeel dat er altijd dient te worden gescand van het originele papieren proces-verbaal omdat anders de deur wijd open staat

voor het scannen van stukken waarvan achteraf niet meer kan worden vastgesteld of het de originele stukken waren. In reactie op dit advies wordt opgemerkt dat bij de omzetting het proces-verbaal uitgegaan moet worden van het oorspronkelijk opgemaakte origineel. In het geval politiekorpsen zelf het originele proces-verbaal bewaren en een kopie daarvan aan het openbaar ministerie verzenden betreft dit tot op heden een als kopie conform getekend proces-verbaal. Dit kopie conform getekende proces-verbaal kan worden omgezet in een digitaal afschrift en, conform deze regeling, worden voorzien van een elektronische handtekening als waarmerk. Zodra de voortgaande automatisering in de strafprocesketen daartoe de mogelijkheid biedt kunnen de tussenliggende print- en digitaliseringactiviteiten vervallen zodat uiteindelijk de beoogde eindsituatie ontstaat, waarbij in de strafrechtsketen uitsluitend gebruik wordt gemaakt van een proces-verbaal in elektronische vorm terwijl steeds een elektronische handtekening de authenticiteit en integriteit van het proces-verbaal waarborgt.

Tenslotte vraagt de NOvA zich af op welke wijze kan worden vastgesteld dat een digitaal afschrift geen identieke weergave vormt van het papieren proces-verbaal. Voor een toelichting op de vraag op welke wijze kan worden vastgesteld dat een digitaal afschrift geen identieke weergave vormt van een papieren proces-verbaal kan worden verwezen naar de toelichting bij artikel 6, vijfde lid, van het ontwerpbesluit.

Toelichting per artikel

Artikel 1 (begripsomschrijvingen)

Onderdeel a

Voor een omschrijving van het begrip elektronisch proces-verbaal wordt verwezen naar de artikelen 152 en artikel 153, tweede lid, van het Wetboek van Strafvordering. Op grond van artikel 153, tweede lid, tweede volzin van het Wetboek van Strafvordering wordt met een ondertekend proces-verbaal gelijkgesteld een proces-verbaal dat langs elektronische weg is opgemaakt, mits dit voldoet aan de bij of krachtens algemene maatregel van bestuur gestelde eisen. Dit betreft de wijze waarop processen-verbaal als bedoeld in artikel 152 van het Wetboek van Strafvordering moeten worden opgemaakt. Het gaat dus om processen-verbaal die door opsporingsambtenaren moeten worden opgemaakt «van het door hen opgespoorde strafbare feit of van hetgeen door hen tot opsporing is verricht of bevonden». Dit besluit bevat die eisen. De eisen hebben betrekking op een proces-verbaal dat langs elektronische weg is opgemaakt of dat langs elektronische weg is omgezet in een digitaal afschrift.

Onderdeel b

Een digitaal afschrift van een proces-verbaal is het resultaat van het scannen van een papieren proces-verbaal. Door middel van het scannen wordt een papieren proces-verbaal, dat door een opsporingsambtenaar is ondertekend, omgezet in een elektronisch gegevensbestand Ook de handtekening van de opsporingsambtenaar op het papieren proces-verbaal wordt dus gescand. Het elektronische gegevensbestand vormt een digitaal afschrift van het papieren proces-verbaal, dat vooral is bedoeld om vanaf een beeldscherm te kunnen worden gelezen. De term digitaal afschrift wordt gebruikt om aan te geven dat het gaat om een met behulp van scannen vervaardigd afschrift in elektronische vorm. Dit proces moet worden onderscheiden van het kopiëren, waarbij van het papieren proces-verbaal een eveneens papieren afschrift of kopie wordt

vervaardigt. Een digitaal afschrift kan wordt uitgeprint, de gescande handtekening is dan eveneens zichtbaar.

Deze algemene maatregel van bestuur geeft regels over zowel het proces-verbaal dat in elektronische vorm wordt opgesteld als het papieren proces-verbaal dat in elektronische vorm wordt omgezet, omdat in beide gevallen sprake is van een elektronisch proces-verbaal. Om de betrouwbaarheid en integriteit van het elektronisch proces-verbaal te waarborgen is een elektronische handtekening vereist. Een digitaal afschrift, dat is voorzien van een geldige elektronische handtekening, wordt aangemerkt als een elektronisch proces-verbaal in de zin van deze algemene maatregel van bestuur.

Onderdeel c

De validatie betreft de vaststelling van de geldigheid van een elektronische handtekening. Dit valt in twee onderdelen uitéén.

Een geldig certificaat waarborgt dat een document door een bepaalde persoon is opgesteld (authenticiteit). Dit is een elektronisch bestand, dat gegevens bevat aan de hand waarvan de geldigheid van de elektronische handtekening kan worden geverifieerd. Dit betreft personalia en eventueel ook gegevens over de functie, de instantie of organisatie waartoe de ondertekenaar behoort en andere relevante gegevens. De geldigheid van het certificaat op het moment van ondertekening wordt vastgesteld aan de hand van gegevens van het certificaat, aangevuld met gegevens van de certificatiedienstverlener. Dit betreft persoonsgegevens en eventueel ook functiegegevens, instantiegegevens en andere relevante gegevens. De meest gangbare toepassingen waarmee documenten kunnen worden ingelezen voeren deze certificaatcontroles automatisch uit. De leveranciers van deze toepassingen (e-mail-, tekstverwerking- en leestoepassingen) leveren bij hun hard- en softwareproducten gegevens over de betrouwbaarheid van certificaten en certificatiedienstverleners.

Een zogenaamde hash-waarde, in combinatie met een elektronische handtekening, wordt gebruikt om na te gaan of een document ongewijzigd is nadat dit is ondertekend (integriteit). Een hash-waarde kan worden omschreven als een wiskundige functie die als invoer een bitstring van een willekeurige lengte heeft, en als uitvoer een bitstring van een vaste lengte. Bij iedere afwijking, gebruik of andere mutatie van het document verandert de hash-waarde. Bij het inlezen van het document worden automatisch de hash-waarde van het document berekend en vergeleken met de door middel van de publieke sleutel ontsleutelde ondertekening die aan het elektronische document is gehecht. Als de hash-waarden identiek zijn dan betekent dit dat het document ongewijzigd is gebleven.

Onderdeel d

Voor een omschrijving van het begrip elektronische handtekening wordt verwezen naar artikel 3:15a, vierde lid, van het Burgerlijk Wetboek. In dat artikel wordt onder een elektronische handtekening verstaan een handtekening die bestaat uit elektronische gegevens die zijn vastgehecht aan of logisch geassocieerd zijn met andere elektronische gegevens en die worden gebruikt als middel voor authentificatie. Een elektronische handtekening betreft geen op zichzelf staande set van gegevens, er is sprake van een combinatie van twee groepen elektronische gegevens. De ene groep van gegevens dient, vanwege de band met de andere gegevens, gebruikt te kunnen worden voor authentificatie. De termen authentificatie en authenticatie worden binnen de informatiebeveiliging

gebruikt om hetzelfde aan te duiden, te weten het proces waarmee met bepaalde zekerheid de identiteit van een persoon of computer vastgesteld wordt.

Onderdeel e

Onder een gekwalificeerde handtekening wordt verstaan een elektronische handtekening gebaseerd op een gekwalificeerd certificaat en gegenereerd door een veilig middel voor het aanmaken van elektronische handtekeningen overeenkomstig de eisen, genoemd in artikel 15a, tweede lid, onderdelen a tot en met f, van Boek 3 van het Burgerlijk Wetboek. Voor de toelichting kan worden verwezen naar paragraaf 4 van het algemeen deel van deze toelichting.

Onderdeel f

De elektronische dagtekening is een tijdstempel dat langs elektronische weg wordt geplaatst. Hiermee wordt invulling gegeven aan het wettelijk vereiste dat het proces-verbaal is gedagtekend (art. 153, tweede lid, Sv). Tevens dient de dagtekening om de geldigheid van het gehanteerde certificaat op het moment van de ondertekening, en daarmee de geldigheid van een elektronische handtekening, op een later tijdstip vast te kunnen stellen. Hierop wordt nader ingegaan bij de toelichting op artikel 2, eerste lid.

Onderdeel g

In dit besluit worden enkele begrippen gehanteerd rond de elektronische handtekening, die reeds zijn omschreven in de Telecommunicatiewet. Dit betreft de begrippen certificaat, gekwalificeerd certificaat, certificatiedienstverlener en veilig middel. Deze begrippen worden omschreven in artikel 1.1, onderdelen ss, tt, uu respectievelijk ww, van de Telecommunicatiewet.

Onderdeel h

In dit besluit worden verplichtingen opgelegd over het opmaken, verzenden en bewaren van een elektronisch proces-verbaal of een digitaal afschrift. In het ontwerpbesluit, dat in consultatie is gegeven, was in artikel 2, tweede lid, geregeld dat een digitaal afschrift wordt voorzien van een elektronische handtekening van een daartoe aangewezen ambtenaar als waarmerk. In artikel 6, eerste lid, was de verplichting opgenomen om, na de ontvangst van een elektronisch proces-verbaal, onmiddellijk een bevestiging van ontvangst te verzenden. In hun adviezen over het ontwerpbesluit hebben de Raad voor de rechtspraak en de Nederlandse Vereniging voor Rechtspraak erop gewezen dat niet duidelijk was wie de betreffende maatregelen moest treffen.

Een elektronisch proces-verbaal kan worden opgemaakt door een opsporingsambtenaar die beschikt over de mogelijkheid een elektronische handtekening te plaatsen, De opsporingsambtenaren zijn aangewezen in de artikelen 141 en 142 van het Wetboek van Strafvordering. Dit betreft ambtenaren van politie, militairen van de Koninklijke marechaussee, officieren van justitie, opsporingsambtenaren van bijzondere opsporingsdiensten en buitengewoon opsporingsambtenaren. Aldus kan de organisatie, waar een opsporingsambtenaar werkzaam is, een regionaal politiekorps zijn, de Koninklijke marechaussee, de rijksrecherche, een bijzondere opsporingsdienst, een parket of een vakdepartement. De verplichtingen over de inrichting van het certificaat en de bewaring en beveiliging van gegevens, uitgewerkt in de artikelen 3, 5 en 7, zijn dan

gericht tot het hoofd van de betreffende organisatie. Ditzelfde geldt voor de verplichting om te voorzien in een geldig elektronisch proces-verbaal (artikel 6, zesde lid).

Een digitaal afschrift kan worden vervaardigd door een ambtenaar die is belast met het scannen van processen-verbaal. Dit betreft ambtenaren van een politiekorps, van het openbaar ministerie of van een rechterlijke instantie. De verplichtingen over het aanwijzen van een ambtenaar, de omzetting van een papieren proces-verbaal in een digitaal afschrift, uitgewerkt in de artikelen 2, tweede lid en 4, zijn dan gericht tot het hoofd van de betreffende organisatie. Ditzelfde geldt voor de verplichting om te voorzien in een geldig digitaal afschrift (artikel 6, zesde lid).

Een elektronisch proces-verbaal of een digitaal afschrift kan worden ontvangen door een ambtenaar die werkzaam is bij het openbaar ministerie of bij een rechterlijke instantie. De verplichtingen tot het verzenden van een bevestiging van ontvangst, de validatie van een elektronisch proces-verbaal en de beveiliging van gegevens, uitgewerkt in de artikelen 6 en 7, zijn dan gericht tot het hoofd van de betreffende organisatie.

Artikel 2 (eisen elektronisch proces-verbaal)

Dit artikel vormt de kern van dit besluit, omdat hierin de eisen zijn vastgelegd die gelden voor de gelijkstelling van een elektronisch proces-verbaal met een papieren proces- verbaal, op grond van artikel 153, tweede lid, van het Wetboek van Strafvordering.

In Richtlijn 1999/93/EG, van 13 december 1999[1], zijn regels gegeven voor de elektronische handtekening. De richtlijn beoogt regels te geven voor de elektronische handtekening in het belang van de ontwikkeling van de elektronische communicatie en de elektronische handel. De richtlijn is geïmplementeerd met de Wet elektronische handtekeningen die in 2004 in werking is getreden. De Wet elektronische handtekeningen voorzag in de wijziging van het Burgerlijk Wetboek, de Telecommunicatiewet, de Wet Onafhankelijke post- en telecommunicatieautoriteit en de Wet op de economische delicten. Dit met het oog op het stellen van voorwaarden waaronder de elektronische handtekening ten behoeve van vermogensrechtelijke betrekkingen en handelingen wordt gelijkgesteld aan de handgeschreven handtekening. De belangrijkste bestanddelen van de wettelijke regeling zijn terug te vinden in artikel 3:15a van het Burgerlijk Wetboek en de artikelen 18:15 tot en met 18.18 Van de Telecommunicatiewet.

De elektronische handtekening die aan de eisen van artikel 3:15a, tweede lid, onderdelen a tot en met f van het Burgerlijk Wetboek voldoet, wordt aangeduid als de gekwalificeerde elektronische handtekening. Essentieel zijn het gebruik van een gekwalificeerd certificaat en van een veilig middel. Een gekwalificeerd certificaat dient bepaalde informatie te bevatten (art. 18.15, tweede lid, Tw). Dit betreft onder meer de identificatie van de certificatiedienstverlener, de naam van de ondertekenaar, de gegevens voor het verifiëren van de handtekening, de vermelding van de geldigheidsduur van het certificaat en de elektronische handtekening van de certificatiedienstverlener (art. 3 Besluit elektronische handtekeningen). Een certificaat wordt uitgegeven door een certificatiedienstverlener. Certificatiedienstverleners moeten zijn geregistreerd bij de Onafhankelijke Post- en Telecommunicatieautoriteit (OPTA). Nederland kent diverse bevoegde certificatiedienstverleners. De OPTA heeft hiervan een lijst beschikbaar.

[1] Pb L 13/12.

De aan de certificatiedienstverlener en het gekwalificeerde certificaat te stellen eisen zijn uitgewerkt in het Besluit elektronische handtekeningen. In de Regeling elektronische handtekeningen is hieraan verdere uitwerking gegeven, aan de hand van de specificaties van ETSI[1]. Het voldoen aan deze specificaties is echter niet verplicht; een certificatiedienstverlener kan zelf bepalen op welke wijze hij aantoont dat aan de wettelijke eisen wordt voldaan. Het voldoen aan de ETSI-specificaties is echter wel voldoende voor het vermoeden dat aan de eisen van het besluit wordt voldaan. Onze Minister van Economische Zaken kan organisaties aanwijzen die bevoegd zijn certificatiedienstverleners te toetsen op overeenstemming met de bij of krachtens de wet gestelde eisen (art. 18.16 Tw).

De eisen voor het veilige middel voor het aanmaken van elektronische handtekeningen zijn eveneens uitgewerkt in het Besluit elektronische handtekeningen. Via passende technieken en procedures dient het veilige middel tenminste te waarborgen dat de gegevens voor het aanmaken van handtekeningen in de praktijk slechts één keer kunnen voorkomen en de vertrouwelijkheid daarvan redelijkerwijs gegarandeerd is, dat die gegevens niet kunnen worden afgeleid en de handtekening beschermd is tegen vervalsing. In de Regeling elektronische handtekeningen is hieraan verdere uitwerking gegeven, aan de hand van een specificatie van het CEN Workshop Agreement[2]. Een veilig middel wordt vermoed te voldoen aan de vereisten van artikel 5 van het Besluit elektronische handtekeningen indien aan die specificatie wordt voldaan. De overeenstemming van veilige middelen met de vereisten van de richtlijn (bijlage III) wordt vastgesteld door een door een daarvoor geaccrediteerde instelling die onafhankelijk is van de betrokken partijen[3]. Inmiddels heeft Onze Minister van Economische Zaken twee bevoegde instellingen aangewezen.

Eerste lid

In dit lid zijn de eisen neergelegd voor een elektronisch proces-verbaal.

De belangrijkste eis is dat het proces-verbaal is voorzien van een gekwalificeerde elektronische handtekening. Dit betekent dat voor de elektronische handtekening gebruik wordt gemaakt van een gekwalificeerd certificaat en van een veilig middel.

Het certificaat, dat wil zeggen een elektronisch bestand, en het veilig middel, dat wil zeggen een smartcard of USB-token, worden door de certificatiedienstverlener in persoon uitgereikt aan een opsporingsambtenaar die daardoor in staat is een elektronische handtekening te plaatsen op het proces-verbaal. De elektronische handtekening wordt geplaatst door de smartcard in te voeren in een reader of de USB-token in te voeren in de USB-poort van een computer. Met behulp van een softwareprogramma wordt de elektronische handtekening aan een elektronisch bestand gekoppeld (PDF). Het bestand kan worden geopend met behulp van een sofwareprogramma (bijvoorbeeld Adobe), dat tevens de mogelijkheid biedt om de geldigheid van de handtekening te verifiëren.

Het is te verwachten dat in de dagelijkse praktijk een belangrijke rol zal toekomen aan de werkgever van de betreffende ambtenaar bij het faciliteren van de afgifte van certificaat of veilig middel. Dit hangt samen met het feit dat de kosten van de verstrekking van het certificaat of het veilig middel voor rekening van de beheerder zullen komen. De faciliterende rol van de beheerder zal echter ook tot uitdrukking kunnen komen in de procedure rond het aanvragen of intrekken van een certificaat. Het ligt voor de hand dat de beheerder als werkgever op deze terreinen namens de opsporingsambtenaar optreedt.

[1] Dit betreffen de specificaties ETSI TS 101 456 en 101 862 (artikelen 2 en 3 Regeling elektronische handtekeningen).
[2] Dit betreft de specificatie CEN Workshop Agreement 14169 (art. 4 Regeling elektronische handtekeningen).
[3] Dit betreft de norm EN 45011 (art. 5 Regeling elektronische handtekeningen).

Aanvullend geldt het vereiste van een elektronische dagtekening. Deze is van belang om op geautomatiseerde wijze de geldigheid van het certificaat van een elektronische handtekening ook op een later moment te kunnen vaststellen. Hierbij gaat het om de geldigheid van het certificaat op het moment dat het werd gebruikt voor de ondertekening. Het moment van publicatie van de intrekking van een certificaat kan namelijk enkele uren later zijn dan het moment van het verzoek daartoe. In de Regeling elektronische handtekeningen wordt als eis gesteld dat de tijdsduur tussen het ontvangen van een verzoek tot intrekking van een gekwalificeerd certificaat en de publicatie van die intrekking maximaal 24 uur mag zijn, in overeenstemming met de ETSI norm TS 101 456. Het kan dus zijn dat een certificaat op het moment van het gebruik feitelijk als ingetrokken moet worden beschouwd, maar dat dit nog niet vastgesteld kan worden omdat de publicatie van de intrekking nog niet heeft plaatsgevonden. De dagtekening dient dan als bewijs voor het moment van de ondertekening waarmee enige uren (of dagen) nadien alsnog kan worden vastgesteld of het certificaat geldig was op het moment van die ondertekening. Er zijn diverse dienstverleners, waaronder certificatiedienstverleners, die «vertrouwde tijdstempels» afgeven. Een «vertrouwd tijdstempel» wordt uitgegeven door een «tijdstempel autoriteit» (Timestamp Authority of TSA) die de juistheid van het tijdstempel garandeert.

Voorts worden eisen gesteld aan het documentformaat waarin het elektronisch proces-verbaal wordt opgesteld. Dit is van belang voor de verdere verwerking van het proces-verbaal binnen de strafrechtsketen en voor de archivering. Indien de verschillende instanties binnen de keten verschillende documentformaten hanteren dan zal dit de mogelijkheid tot het langs elektronische weg kunnen uitwisselen van de gegevens ernstig kunnen belemmeren. Om hierin de gewenste eenduidigheid te creëren is aangesloten bij de regels van de Archiefwet 1995. Uitgangspunt van de Archiefwet 1995 is dat documenten dienen te worden bewaard in de vorm waarin ze zijn aangeleverd. De Archiefregeling schrijft voor dat digitale archiefbescheiden worden opgeslagen in een valideerbaar en volledig gedocumenteerd bestandsformaat dat voldoet aan een open standaard, tenzij die redelijkerwijs niet van de zorgdrager kan worden verwacht (art. 26, eerste lid, Archiefregeling).[1]

Van belang is dat er standaarden worden gebruikt voor het bewaken van de integriteit van geavanceerde elektronische documenten voor de lange termijn (meer dan tien jaar). Hiervoor zijn inmiddels Europese standaarden gedefinieerd zoals XAdES (ETSI 1010 903, voor XML, in het bijzonder XadES-A) of PAdES (ETSI TS 102 778, voor PDF) en LTANS[2] of de ANSI X9.95 (voor evidence records). Deze standaarden, of gelijksoortige standaarden, verdienen de voorkeur.

In de adviezen van de Raad voor de rechtspraak en de Nederlandse Vereniging voor Rechtspraak is de vraag opgeworpen of het mogelijk is dat meerdere opsporingsambtenaren een elektronisch proces-verbaal ondertekenen. Dit is inderdaad het geval. Als de betreffende opsporingsambtenaren in staat zijn een elektronische handtekening te plaatsen, overeenkomstig de eisen van dit besluit, dan kunnen zij het proces-verbaal tevens ondertekenen,

Tweede lid

Dit besluit voorziet tevens in regels voor de omzetting van het papieren proces-verbaal in een digitaal afschrift, dat als zelfstandig bewijsmiddel kan dienen in de zin van artikel 344, eerste lid, onderdeel 2°, van het Wetboek van Strafvordering. In het algemeen deel is reeds opgemerkt dat bij de parketten voorzieningen zijn ingericht voor het langs elektronische weg omzetten van een papieren proces-verbaal in een digitaal afschrift.

[1] In de Justitie standaardisatierichtlijnen voor digitale bestanden is de PDF/A1-standaard (portable document format/archiving) als eis voor digitale archivering vastgelegd. Dit betreft een onderverdeling van PDF, dat bewaring voor langere termijn mogelijk maakt. De ontwikkelingen ten aanzien van het gebruik van XML gebaseerde formaten moet echter niet verhinderd worden omdat ook XML gebaseerde documenten archiefwaardig kunnen zijn.

[2] Long Term Archive and Notary Services (LTANS) http://www.ietf.org/dyn/wg/charter/ltans-charter.html

Dit vindt plaats door middel van het scannen van het proces-verbaal. Het scannen van een proces-verbaal levert in principe een identieke weergave op die zelfstandig als bewijsmiddel kan dienen. Het resultaat van het scanproces wordt in dit besluit aangeduid als «een digitaal afschrift». Het digitaal afschrift kan zelfstandig als bewijsmiddel dienen als voldaan wordt aan de eisen van dit besluit.

Een essentieel vereiste betreft het gebruik van een gekwalificeerde elektronische handtekening als waarmerk. De betekenis van de handtekening als waarmerk is dat degene die de handtekening heeft geplaatst er voor in staat dat het in elektronisch vorm omgezette proces-verbaal een identieke weergave vormt van het originele papieren proces-verbaal. Niet vereist is dat degene die is belast met het scannen van het proces-verbaal een opsporingambtenaar is. De voorgestelde inrichting van het scanproces neemt deze noodzaak weg. Aldus kan een papieren proces-verbaal later worden omgezet in een elektronisch proces-verbaal. De betekenis van deze mogelijkheid voor de efficiency van de strafrechtsketen is van groot belang, omdat het scannen de mogelijkheid biedt om eventuele verschillen op het gebied van de invoering en het gebruik van een elektronische handtekening binnen de strafrechtsketen te herstellen. Als een opsporingsambtenaar niet in staat is een elektronisch proces-verbaal in te sturen, bijvoorbeeld omdat hij niet beschikt over een geldig gekwalificeerd certificaat of een veilig middel, dan kan hierin ook worden voorzien door het papieren proces-verbaal te scannen en te voorzien van een gekwalificeerde elektronische handtekening als waarmerk. Een dergelijke omzetting kan bij de politie zelf worden verricht maar tevens bij het openbaar ministerie of de zittende magistratuur, overeenkomstig de eisen van dit besluit.

Artikel 3 (eisen certificaat)

Een certificaat wordt door een certificatiedienstverlener aan de aanvrager afgegeven. De certificatiedienstverlener stelt de identiteit van de persoon, die in het certificaat als ondertekenaar wordt aangeduid, vast voordat het certificaat wordt afgegeven (art. 18:15 Tw). Hieraan kan worden voldaan doordat de aanvrager fysiek verschijnt voor een medewerker van een certificatiedienstverlener en een echt, eigen, geldig en gekwalificeerd identiteitsbewijs overlegt. Een certificaat kan onafhankelijk van een veilig middel worden uitgegeven. De in een certificaat op te nemen informatie is vastgelegd in het Besluit elektronische handtekeningen. Dit betreft onder meer gegevens over de ondertekenaar, de certificatiedienstverlener, de verificatie van de handtekening, de geldigheidsduur en eventuele beperkingen in het gebruik van het certificaat (artikel 3 Besluit elektronische handtekeningen).

Een opsporingsambtenaar kan zelfstandig een certificaat aanvragen bij de certificatiedienstverlener maar de wet staat niet in de weg dat door of namens de korpsbeheerder een certificaat wordt aangevraagd. Ditzelfde geldt voor de intrekking van een certificaat; een verzoek daartoe kan worden gedaan door de ondertekenaar of door een door hem aangewezen persoon of instantie (art. 2, onderdeel k, Besluit elektronische handtekeningen). Dit betekent dat door of namens de korpsbeheerder verzocht kan worden om intrekking van een certificaat. Op dit punt zijn in dit besluit geen aanvullende regels opgenomen. Een uitzondering wordt gevormd door de gegevens die in het certificaat worden opgenomen.

Eerste lid

In het certificaat moeten gegevens worden opgenomen over de organisatie waar de ambtenaar, aan wie het certificaat is afgegeven, werkzaam is. Op een opsporingsambtenaar rust de verplichting om in bepaalde omstandigheden een proces-verbaal op te maken (art. 152 Sv). De opsporingsambtenaren zijn aangewezen in de artikelen 141 en 142 van het Wetboek van Strafvordering. Dit betreft ambtenaren van politie, militairen van de Koninklijke marechaussee, officieren van justitie, opsporingsambtenaren van bijzondere opsporingsdiensten en buitengewoon opsporingsambtenaren. Aldus kan de organisatie, waar een opsporingsambtenaar werkzaam is, een regionaal politiekorps zijn, de Koninklijke marechaussee, de rijksrecherche, een bijzondere opsporingsdienst, een parket of een vakdepartement. Een digitaal afschrift kan worden vervaardigd door een ambtenaar die is belast met het scannen van processen-verbaal. Dit betreft medewerkers van een politiekorps of van de rechterlijke macht (openbaar ministerie en zittende magistratuur).

De wet en dit besluit stellen geen beperkingen aan de kring van ambtenaren die een elektronische handtekening kunnen plaatsen maar bevatten eisen om te waarborgen dat een elektronisch proces-verbaal tot het bewijs van een strafbaar feit kan dienen. De aanvraag en intrekking van een certificaat voor een elektronische handtekening behoren tot de verantwoordelijkheid van de werkgever en de ambtenaar die bij de betreffende werkgever in dienst is.

Tweede lid

Artikel 3 van het Besluit elektronische handtekeningen geeft een opsomming van de informatie die een certificaat moet bevatten. Dit betreft onder meer de naam van de ondertekenaar of een als zodanig geïdentificeerd pseudoniem. In dit lid is vastgelegd dat, in afwijking van de regeling van artikel 3, onderdeel c, van het Besluit elektronische handtekeningen, slechts in bijzondere gevallen gebruik kan worden gemaakt van een pseudoniem. In hun advies hebben de Raad voor de rechtspraak en de Raad van Korpschefs i.o. erop gewezen dat verbalisanten «anoniem» relateren, zoals bijvoorbeeld gebruikelijk is in een proces-verbaal van observatie. In de jurisprudentie is de mogelijkheid voor opsporingsambtenaren erkend om, onder bepaalde omstandigheden, een proces-verbaal van verbindingen op te stellen waarbij de verbalisanten worden aangeduid met een codenaam of nummer, die of dat binnen de organisatie herleidbaar is tot hun identiteit[1]. Daarbij kan het gaan om een lid van een arrestatie- of observatieteam of een opsporingsambtenaar van een criminele inlichtingen eenheid (CIE). Overigens biedt de Europese richtlijn de lidstaten hiervoor expliciet de uimte (artikel 8, derde lid).

Artikel 4 (eisen digitaal afschrift)

Eerste lid

Een papieren proces-verbaal kan worden gescand zodat dit wordt omgezet in een elektronisch bestand. Het is van belang dat het scannen van een papieren proces-verbaal zorgvuldig plaatsvindt, zodat het elektronische bestand een identieke weergave vormt van het papieren proces-verbaal. Daarvoor is aangesloten bij de bij of krachtens de Archiefwet 1995 gegeven voorschriften. Technische onvolkomenheden en menselijke fouten of vergissingen moeten uitgesloten worden. Voor wat betreft de techniek kan een onjuiste instelling van de scanapparatuur een schadelijke invloed hebben op de leesbaarheid van het digitale afschrift.

[1] HR. 29-04-1997, NJ '97, no. 666: «Gelet op het doel en de strekking van de Wet (van 11 november 1993, Stb. 1993, 603) moet worden aangenomen dat die term (een persoon wiens identiteit niet blijkt) niet omvat verbalisanten wier persoonsgegevens weliswaar niet (volledig) in het door hen opgemaakte proces-verbaal zijn vermeld, maar van wie vaststaat dat het bevoegde, onder een bepaald codenummer bekende, opsporingsambtenaren betreft alsmede tot welk politieonderdeel zij behoren».

Voor wat betreft de menselijke tussenkomst moet uitgesloten worden dat een proces-verbaal niet volledig gescand wordt of dat pagina's ontbreken. Het scanproces dient op zodanig wijze te worden ingericht dat de techniek en menselijke tussenkomst elkaar ondersteunen. In de praktijk zijn hiervoor goede maatregelen en procedures ontwikkeld. Met de bepaling van dit lid wordt beoogd nauw bij de bestaande maatregelen en procedures aan te sluiten.

In het algemeen deel van de nota van toelichting is de Beleidsregel digitale vervanging archiefbescheiden aan de orde gekomen. De elementen van de procesmatige en technische inrichting, die zijn beschreven in de bijlage bij de beleidsregel, zijn mede van belang voor het scannen van papieren processen-verbaal. Deze elementen hebben betrekking op de apparatuur (aanduiding van de gebruikte scanapparatuur), de software (aanduiding softwarepakket, versienummer, releasedatum, leveranciers en zo nodig de geïnstalleerde service pack of patches), de kwaliteitsprocedures (de criteria voor en de frequentie van interne controles). Het scanproces (registratie metadata, controle correctie en zorgvuldige scanning, te hanteren kleurmodel), de kwaliteit van de scan (300 dpi met bitdiepte 24, opslag van het digitale beeld in een gestandaardiseerd kleurenprofiel, bijvoorbeeld sRGB IEC 61966-2-1:1999) en het bestandsformaat (open standaarden die door middel van een formeel en open proces als ISO en NEN vastgesteld worden; voorbeelden zijn TIFF en PDF/A volgens ISO 19005-1).

De Archiefwet 1995 richt zich echter primair op het duurzaam bewaren van archiefstukken, terwijl in de strafprocesketen de aandacht primair uitgaat naar de handhaving van de rechtsgeldigheid van een elektronisch opgemaakt en getekend proces-verbaal en de overige processtukken in het procesdossier. Daarom is ervoor gekozen om de relevante elementen van de bijlage bij de Beleidsregel digitale vervanging archiefbescheiden op te nemen in een bijlage (I) bij het ontwerpbesluit.

Tweede lid

In dit lid is geregeld dat in een digitaal afschrift wordt vermeldt dat het een identieke weergave en kopie is van het (papieren) proces-verbaal. Hiermee wordt tot uitdrukking gebracht dat er zoveel mogelijk wordt gescand op basis van het originele papieren proces-verbaal. Dit is in het belang van een goede leesbaarheid van het digitaal afschrift. Niet uitgesloten is dat een rechtsgeldig opgemaakte kopie van een papieren proces-verbaal, die voldoet aan de eisen die daaraan in de jurisprudentie worden gesteld, wordt gescand. Daarmee is het binnen de strafrechtsketen mogelijk om een digitaal afschrift te vervaardigen van een kopie van een papieren proces-verbaal van een opsporingsambtenaar. Zoals in het algemeen deel opgemerkt, zijn bij het openbaar ministerie scanstraten ingericht voor het scannen van processen-verbaal van de politie. Het is dan aan het openbaar ministerie om de kwaliteit van het scannen te waarborgen. Niet uitgesloten is dat hierover in individuele strafzaken verantwoording moet worden afgelegd. Met de eis dat het originele papieren proces-verbaal wordt bewaard, conform het bij of krachtens de Archiefwet 1995 bepaalde, is verzekerd dat het resultaat van de scan te allen tijde kan worden geverifieerd.

Derde lid

Met dit lid wordt de mogelijkheid geboden om bij ministeriele regeling nadere regels te stellen betreffende de eisen, normen en standaarden voor het omzetten van een proces-verbaal in een digitaal afschrift. Op grond van de ervaring met het scannen van processen-verbaal kan er aanleiding bestaan voor het stellen van nadere regels. Deze eisen kunnen

betrekking hebben op de procedure van het scannen, de gebruikte apparatuur, de toegang tot de ruimte waar het scannen plaatsvindt of de deskundigheid van de betrokken medewerkers.

In aanvulling op hetgeen hierover bij het eerste lid is opgemerkt, kunnen nadere maatregelen worden getroffen om het scanproces met de hoogste mate van zorgvuldigheid plaats te doen vinden. Deze maatregelen kunnen betrekking hebben op de apparatuur (specificaties), de opleiding van de betrokken ambtenaren, de toegang tot de ruimten waar gescand wordt en de controle van het scanproces.

Een belangrijke maatregel vormt de toepassing van het zogenaamde vier ogen principe, waarbij het resultaat van het scannen op leesbaarheid en volledigheid wordt gecontroleerd door een andere ambtenaar dan degene die het scannen heeft verricht. In een dergelijk geval is het wenselijk dat de ambtenaar die de controle heeft verricht, de elektronische handtekening plaatst. Samenvattend gaat het hier over kwaliteitsaspecten ten aanzien van de exclusiviteit, volledigheid, juistheid, integriteit, controleerbaarheid, tijdigheid, beschikbaarheid, functionaliteit en performance.

Artikel 5 (eisen bewaring proces-verbaal)

Eerste lid

Een door een certificatiedienstverlener uitgegeven certificaat heeft een gelimiteerde geldigheidsduur. In de eerste plaats zal het certificaat moeten worden ingetrokken als een opsporingsambtenaar uit dienst treedt. In de tweede plaats is een certificaat niet onbeperkt geldig. Daarvoor wordt door de certificatiedienstverlener doorgaans een termijn aangehouden van ten hoogste drie jaar. In de derde plaats kan de certificatiedienstverlener de dienstverlening beëindigen. De certificatiedienstverlener is gehouden om het beheer van nog geldige certificaten over te dragen aan een andere geregistreerde certificatiedienstverlener. Als deze overdracht echter redelijkerwijs niet mogelijk is dan moet de certificatiedienstverlener alle door hem uitgegeven en op dat tijdstip nog geldige certificaten intrekken (art. 2, onderdeel p, Besluit elektronische handtekeningen)

De certificatiedienstverlener is verplicht informatie over een gekwalificeerd certificaat tenminste zeven jaar te bewaren, na de datum waarop de geldigheid van het certificaat is verlopen (artikel 2, onderdeel i, van het Besluit elektronische handtekeningen). De certificatiedienstverlener is gehouden deze informatie te publiceren gedurende de geldigheid van het gekwalificeerde certificaat en tot ten minste zes maanden na het tijdstip waarop de geldigheid van het certificaat is verlopen of, als dat eerder is, na het tijdstip waarop de geldigheid is beëindigd door intrekking van het certificaat. Daarmee is verificatie door de ontvanger van het ondertekende document gedurende die periode, ook online, mogelijk (artikel 2, onderdeel l, van het Besluit elektronische handtekening).

Deze regeling brengt met zich mee dat mogelijk reeds zes maanden na het verlopen van het certificaat, maar doorgaans tien jaar na de afgifte, het risico bestaat dat niet meer kan worden vastgesteld of het certificaat geldig was op het moment waarop dit werd gebruikt. Daarom wordt in dit lid geregeld dat over de elektronische handtekening en de dagtekening aanvullend de gegevens worden bewaard, die zijn omschreven in de bijlage (II) bij dit besluit.

Het doel van de lijst van gegevens van de bijlage is om aan de gebruikers van het elektronisch proces-verbaal duidelijkheid te bieden over de gegevens die bewaard moeten worden. Deze gegevens worden ofwel op het certificaat vermeld ofwel bij de certificatiedienstverlener bewaard zodat het gaat om een aanvullende bewaarplicht om in een later stadium de geldigheid van de elektronische handtekening, op het moment waarop deze geplaatst werd, aan te kunnen tonen. De uit deze bewaarplicht voortvloeiende beheerslast voor politie en justitie lijkt van beperkte omvang. Op de markt zijn diensten en producten beschikbaar waarvan gebruik gemaakt kan worden. Deze diensten kunnen gemeenschappelijk worden gebruikt door de personen en instanties, die betrokken zijn bij het elektronisch proces-verbaal.

Overwogen kan worden om de lijst van gegevens bij ministeriele regeling vast te stellen omdat dit de mogelijkheid biedt van een flexibele aanpassing als wijziging van de standaarden daartoe aanleiding geeft. Een alternatief is om te volstaan met een algemene bepaling in het besluit en de lijst van gegevens, meer bij wijze van voorbeeld, op te nemen in de nota van toelichting. Vooralsnog is echter gekozen om de voorgestelde lijst van gegevens als bijlage (II) bij dit besluit op te nemen omdat de lijst een afspiegeling vormt van standaarden die in de praktijk reeds gebruikt worden. Het is dan ook niet de bedoeling dat de lijst van de gegevens frequent aangepast wordt maar dat deze gedurende een langere periode zal gelden. Ingeval de standaarden in de loop der tijd toch evolueren of veranderen dan zal dit aanleiding geven tot aanpassing van de lijst.
Het enkele feit dat enige gegevens uit de lijst niet of niet meer bij het betreffende elektronische proces-verbaal aanwezig zijn, leidt evenwel niet bij voorbaat tot ongeldigheid van de elektronische handtekening.

In zijn advies heeft de Raad van Korpschefs voorgesteld om de onderdelen C en D van de bijlage (II) te laten vervallen. Het vastleggen van deze gegevens zou technisch te complex worden, mede in het licht van het doel van de vastlegging, en tot onnodige verzwaring van het gebruik van een elektronisch document leiden. Dit advies is niet overgenomen omdat de gegevens van deze onderdelen nodig zijn op grond van het bij of krachtens de Archiefwet 1995 bepaalde en om ook op termijn de geldigheid van een elektronische handtekening te kunnen aantonen. De betreffende gegevens kunnen overigens op geautomatiseerde wijze worden ingevuld tijdens het proces van de elektronische handtekening. Dit vormt bijvoorbeeld onderdeel van de Waarmerk- Teken- en Validatieservice (WTV-service), waarop hieronder nader worden ingegaan. Er is geen noodzaak tot het handmatig toevoegen van allerlei kenmerken door een gebruiker, zoals de Raad kennelijk veronderstelt.

In zijn advies heeft de Nederlandse Vereniging voor Rechtspraak (NVvR) erop gewezen dat het niet gebruikelijk is in Nederlandse wetgeving gebruik te maken van Engelse termen. Naar aanleiding van dit advies zijn Engelstalige termen zoveel mogelijk toegelicht aan de hand van begrippen van PKI-overheid.

Tweede lid

De gegevens, die zijn omschreven in de bijlage (II) bij dit besluit, worden even lang bewaard als het elektronisch proces-verbaal zelf. Voor de bewaartermijn van het elektronisch proces-verbaal wordt verwezen naar paragraaf 7 van het algemeen deel van deze nota van toelichting, waar sprake is van de onderscheiden selectielijsten op basis van de Archiefwet 1995.

Bij de Justitiële Informatiedienst van het ministerie van justitie is een Waarmerk- Teken- en Validatie-service (WTV-service) ontwikkeld. Dit is een dienst waarmee documenten kunnen worden voorzien van een elektronische handtekening, kunnen worden gewaarmerkt en kunnen worden gevalideerd. Doel van deze dienst is de authenticiteit van documenten vast te leggen het behoud daarvan voor onbepaalde tijd te garanderen. Met behulp van een gecertificeerde PKI-infrastructuur worden elektronische documenten door de gebruiker gewaarmerkt en ondertekend. De WTV-service kan worden gebruikt voor elektronische processen-verbaal. Dit kan een proces-verbaal van een opsporingsambtenaar zijn, of een proces-verbaal dat is gescand door een medewerker van het openbaar ministerie. Daarbij wordt gebruik gemaakt van een gecertificeerde PKI-infrastructuur. Dit betekent dat een opsporingsambtenaar een door de Justitiële Informatiedienst beschikbaar te stellen softwareprogramma kan gebruiken voor het ondertekenen van een elektronisch proces-verbaal. Daarnaast zorgt de WTV-service ervoor dat bepaalde gegevens over de geldigheid van de elektronische handtekening worden verzameld en bewaard zodat de documenten later kunnen worden gevalideerd, ongeacht de beschikbaarheid van de informatie bij de certificatiedienstverlener. De waarde van de documenten als bewijsmiddel blijft dan behouden. Het betreffende document wordt, inclusief de gegevens omtrent de validiteit, duurzaam bewaard in een elektronisch archief.

Derde lid

Het elektronisch proces-verbaal vormt een gegevensbestand dat binnen de strafrechtsketen bewerkt kan worden. Dit is echter niet de bedoeling omdat daardoor de hash-waarde verandert en de geldigheid van de elektronische handtekening in een later stadium niet meer aangetoond kan worden. Het behoeft nauwelijks betoog dat een dergelijke handelwijze afbreuk kan doen aan de betekenis van het elektronisch proces-verbaal als bewijsmiddel. In plaats daarvan dient het elektronisch proces-verbaal in ongewijzigde vorm te worden bewaard, bij voorkeur afgezonderd van de werkprocessen binnen de strafrechtsketen, zodat authenticiteit en integriteit gewaarborgd zijn. Bij de ontwikkeling van GPS wordt rekening gehouden met een centrale opslag van elektronische processen-verbaal.

De verschijningsvorm van het elektronisch proces-verbaal als gegevensbestand biedt voldoende mogelijkheden voor het bewerken van afdrukken van het elektronisch proces-verbaal binnen de strafrechtsketen. In de eerste plaats kan het elektronisch proces-verbaal worden afgedrukt of uitgeprint. Daarna kan de afdruk worden bewerkt, bijvoorbeeld door deze van aantekeningen te voorzien. In de tweede plaats kan het elektronisch proces-verbaal langs elektronische weg worden gekopieerd, waarna het gekopieerde bestand bewerkt kan worden. Dit biedt bijvoorbeeld aan een parketsecretaris de mogelijkheid om in het gekopieerde bestand aantekeningen op te nemen ten behoeve van de behandeling van de strafzaak ter terechtzitting door de officier van justitie. Voorop staat echter dat het elektronisch proces-verbaal in de oorspronkelijke staat wordt bewaard – afgezonderd van de werkprocessen binnen de strafrechtsketen – en te allen tijde kan worden opgevraagd, indien daartoe aanleiding bestaat.

In zijn advies heeft de NvVR de vraag opgeworpen of het mogelijk is om aantekeningen te maken in een digitaal dossier, zonder dat deze aantekeningen voor anderen leesbaar zijn. De NvVR geeft er de voorkeur aan dat deze aantekeningen niet leesbaar zijn voor andere procespartijen. In reactie op deze vraag kan worden opgemerkt dat het niet de bedoeling is dat aantekeningen van bewerkers van een elektronisch proces-verbaal rechtstreeks in het originele gegevensbestand worden aangebracht. Daarmee wordt afbreuk gedaan aan de mogelijkheid om de integriteit en authenticiteit van het elektronisch proces-verbaal in een later stadium vast

te stellen. Wel kan een afzonderlijk elektronisch gegevensbestand worden aangemaakt ten behoeve van eigen gebruik door de behandelende rechters. Daarmee is tevens verzekerd dat de door hen gemaakte aantekeningen slechts ter kennis kunnen komen van degenen die geautoriseerd zijn tot kennisneming van de gegevens van dit bestand. Dit element houdt geen verband met de betrouwbaarheid van het elektronisch proces-verbaal als wettig bewijsmiddel en is niet in deze algemene maatregel van bestuur betrokken.

In zijn advies heeft de NVvR tevens vragen gesteld over de betekenis van de hash-waarde voor de rechtspraktijk. Deze vragen nopen tot een korte toelichting op de betekenis die de hash-waarde heeft in relatie tot de elektronische handtekening en daarmee de waarborging van de authenticiteit en integriteit van het elektronische proces-verbaal. Technische gezien behelst het waarborgen van de authenticiteit en integriteit van een document dat met het certificaat of middel dat de ondertekenaar ter beschikking staat, de door de computer berekende hash-waarde van het document wordt versleuteld en dat deze versleutelde hash-waarde tezamen met persoonsidentificerende gegevens aan het document worden gehecht. Daarmee wordt het document van een zogeheten «fingerprint» voorzien die afhankelijk van het doel waarvoor deze aan het document wordt gehecht, behalve als een elektronische handtekening ook als een elektronisch waarmerk kan fungeren. De integriteit van het document kan worden vastgesteld doordat (met de meeste van de gangbare toepassingen) bij het openen van een document op de achtergrond automatisch een hash-waarde berekening wordt uitgevoerd en het resultaat hiervan wordt vergeleken met de alsdan ontsleutelde hash-waarde die met het elektronische document (in versleutelde vorm) is meegegeven. Als de hash-waarden identiek zijn dan betekent dit dat het document ongewijzigd is gebleven. De informatie over de uitkomsten van deze validatie worden door de gangbare toepassingen automatisch gegenereerd. De authenticiteit van het document kan door de persoon die het document opent worden vastgesteld op grond van de informatie die het certificaat met de «fingerprint» heeft meegeleverd. In artikel 3 van dit Besluit is omschreven welke gegevens in het certificaat moeten zijn opgenomen en dus met de «fingerprint» worden meegeleverd.
Uiteraard is mogelijk een bundel documenten, die tezamen het strafdossier vormen, te voorzien van «fingerprint». De betekenis van deze «fingerprint» is echter een andere dan de «fingerprint» die als elektronische handtekening of als elektronisch waarmerk is verbonden is aan het proces-verbaal en aan andere afzonderlijke authentieke documenten van het strafdossier.

De bewaring vindt overigens plaats op grond van de artikelen 11, 12, en 13 van het Archiefbesluit 1995, meer specifiek uitgewerkt in de Archiefregeling.

Artikel 6 (validatie)

Dit artikel bevat regels voor de verzending en ontvangst van een elektronisch proces-verbaal aan en van een andere persoon of instantie binnen de strafrechtsketen. Deze regels hebben ten doel de authenticiteit en integriteit van een elektronisch proces-verbaal binnen de strafrechtsketen te waarborgen.

Eerste lid

In dit lid is de verplichting vastgelegd dat na de ontvangst van een elektronisch proces-verbaal onverwijld een bevestiging van ontvangst wordt verzonden aan de persoon of instantie die dit proces verbaal heeft

verzonden. Het ligt voor de hand dat deze bevestiging van ontvangst langs elektronische weg wordt verzonden.

Tweede lid

De bevestiging van ontvangst wordt bewaard door de ontvanger van de bevestiging, dat wil zeggen de persoon of instantie die het elektronisch proces-verbaal heeft verzonden. De bewaarperiode is vastgesteld op vijf jaar. Met dit ontvangstbewijs kan de verzender aantonen dat het proces-verbaal in goede orde bij de ontvanger is aangekomen. Dit is een gevolg van het «langs elektronische weg» verzenden van het proces-verbaal. Een door de politie opgestuurd proces-verbaal zal doorgaans binnen een redelijke termijn door het openbaar ministerie worden beoordeeld. Een bewaarperiode van vijf jaar lijkt voldoende om hierover uitsluitsel te kunnen geven.

Derde lid

In dit lid is vastgelegd dat een elektronisch proces-verbaal, nadat dit is ontvangen van een persoon of instantie die het heeft verzonden, door de ontvangende persoon of instantie wordt gevalideerd. De validatie omvat de verificatie van de geldigheid van het certificaat op het moment van ondertekening en de verificatie van de ongewijzigde staat van het elektronisch proces-verbaal aan de hand van de ondertekening. Doorgaans wordt een dergelijke controle geautomatiseerd uitgevoerd en is menselijke tussenkomst hiervoor niet noodzakelijk.

Vierde lid

De regels over de validatie dienen rekening te houden met de mogelijkheid dat het resultaat daarvan negatief is, dat wil zeggen dat de hash-waarden niet identiek zijn. Indien de validatie zou uitwijzen dat de hash-waarden niet overeenkomen dan heeft kennelijk een bewerking plaatsgevonden nadat de elektronische handtekening geplaatst is. De elektronische handtekening heeft dan zijn geldigheid verloren. In een dergelijk geval is het aangewezen dat de verzendende persoon of instantie hiervan onverwijld in kennis wordt gesteld, zodat deze de nodige maatregelen kan treffen om te voorzien in een elektronisch proces-verbaal, overeenkomstig de eisen van dit besluit.

Vijfde lid

De regels over de validatie nopen tevens tot het onder ogen zien van de situatie dat een digitaal afschrift geen identieke weergave vormt van het originele papieren proces-verbaal. Gedacht kan worden aan de mogelijkheid dat het digitale afschrift niet goed leesbaar is, doordat letters of leestekens tijdens het scannen geheel of gedeeltelijk zijn weggevallen, of dat dit niet volledig is, doordat pagina's van het proces-verbaal niet of niet volledig zijn gescand of als elektronisch bestand zijn weggeschreven. De regels voor het scannen van processen-verbaal van dit besluit zijn er juist op gericht om te voorkomen dat een dergelijke mogelijkheid zich daadwerkelijk voordoet. Niettemin is het niet bij voorbaat uit te sluiten dat, tengevolge van technische onvolkomenheden of menselijke fouten of vergissingen, het digitaal afschrift geen identieke weergave vormt van het originele papieren proces-verbaal. In een dergelijk geval dient dit onverwijld te worden bericht aan de betreffende persoon of instantie, zodat deze de nodige maatregelen kan treffen om te voorzien in een digitaal afschrift, overeenkomstig de eisen van dit besluit.

Zesde lid

In dit lid is vastgelegd dat de persoon of instantie, die een elektronisch proces-verbaal heeft verzonden en aan wie een bericht is verzonden dat de gecontroleerde waarden niet overeen komen of dat een digitaal afschrift geen identieke weergave vormt van het proces-verbaal, gehouden is te voorzien in een elektronisch proces-verbaal, dat is opgemaakt conform de eisen van dit besluit. In de praktijk zal dit betekenen dat de betrokken opsporingsambtenaar het elektronisch proces-verbaal controleert, vaststelt waar het verschil in de hash waarden op is terug te voeren en het al dan niet gecorrigeerde elektronisch proces-verbaal opnieuw ondertekent met behulp van een elektronische handtekening, overeenkomstig de eisen van dit besluit. Als het gaat om een digitaal afschrift van een papieren proces-verbaal, dan is het aangewezen dat de betrokken ambtenaar het digitaal afschrift controleert, vaststelt waar het verschil in de hash waarden op is terug te voeren en het al dan niet gecorrigeerde digitaal afschrift opnieuw voorziet van een elektronische handtekening als waarmerk, overeenkomstig de eisen van dit besluit.

Artikel 7 (beveiliging en toegang tot de gegevens)

Eerste lid

Dit lid bevat een algemene verplichting voor de beheerder om het elektronisch proces-verbaal en de gegevens van het digitaal afschrift, het certificaat en de validatie te beveiligen tegen misbruik, verlies of onrechtmatige verwerking. Deze verplichting strekt ertoe dat een passend beveiligingsniveau gewaarborgd is, gelet op de risico's die de verwerking en de aard van de gegevens met zich meebrengen. Uitgangspunt is dat de regels voor de beveiliging van een papieren proces-verbaal ook van toepassing zijn op een elektronisch proces-verbaal of een afdruk daarvan.

De Regeling informatiebeveiliging politie geeft regels over de beveiliging van informatiesystemen binnen de Nederlandse politie (Regeling van 17 maart 1997, Stcrt. 60). Op grond van deze regeling is de korpsbeheerder gehouden een informatiebeveiligingsbeleid vast te stellen in een beleidsdocument en dit beleid uit te dragen (art. 3, eerste lid). Verder dient voor ieder informatiesysteem een analyse te worden uitgevoerd, aan de hand van de als bijlage bij de regeling opgenomen betrouwbaarheidscriteria en -normklassen (artikel 4, eerste lid). Ter uitvoering van deze regeling is een stelsel voor informatiebeveiliging uitgewerkt, dat onder meer een leidraad Organisatie van de informatiebeveiliging en het «basisbeveiligingsniveau Nederlandse politie» omvat. Daarnaast is de korpsbeheerder op grond van de WPG verplicht passende technische en organisatorische maatregelen te treffen om de politiegegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau, gelet op de risico's die de verwerking en de aard van de politiegegevens met zich meebrengen (art. 4, derde lid, WPG).

Voor het openbaar ministerie en de bijzondere opsporingsdiensten zijn regels voor de beveiliging van gegevens vastgelegd in het Besluit voorschrift informatiebeveiliging rijksdienst 2007 (Vir) en het Besluit voorschrift informatiebeveiliging rijksdienst – bijzondere informatie (Vir-bi). Daarnaast is het College van procureurs-generaal verplicht om passende technische en organisatorische maatregelen te treffen om de strafvorderlijke gegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking, en een passend beveiligingsniveau te

garanderen, in het licht van de stand van de techniek en de kosten van de tenuitvoerlegging (art. 7, eerste lid, j.o. art. 39c WJSG).

Tweede lid

Met dit lid wordt de toegang tot het elektronisch proces-verbaal en de gegevens van het digitaal afschrift, het certificaat en de validatie gebonden aan een voorafgaande autorisatie door de beheerder van de gegevens. Hiermee wordt aangesloten bij de Wet politiegegevens, waarin is bepaald dat de verantwoordelijke voor politiegegevens een systeem van autorisaties onderhoudt, dat voldoet aan de vereisten van zorgvuldigheid en evenredigheid (art. 6, eerste lid, WPG). Met de eis van autorisatie wordt beoogd de toegang tot deze gegevens te beperken tot bepaald aangewezen personen binnen de betreffende organisatie, voor zover dat nodig is voor een goede uitvoering van hun taak. De autorisaties zullen gekoppeld worden aan een bepaalde functie. Het ligt voor de hand om de autorisaties schriftelijk vast te leggen, maar dit is niet vereist. De autorisaties zullen ook langs elektronische weg verleend kunnen worden, zodat de toegang tot de gegevens kan worden verkregen door middel van een gebruikersnaam en een wachtwoord.

De Minister van Veiligheid en Justitie,
I. W. Opstelten